Numbers and Sets

January 13, 2022

Contents

0 Introductory Remarks

The course consists of these notes; there is no *need* to look at any books, but it may be of some use.

There will be 4 example sheets for this course.

1 Proofs

Definition (Proof)**.** A proof is a sequence of true statements without logical gaps, establishing some conclusion.

We have to start somewhere, and have agreed assumptions (axioms).

We want to prove things because:

— We want to know they are true;

— We hope to gain insight into why they are true;

— We might be lucky and the proof is beautiful.

1.1 Examples of statements

(1) There are infinitely many primes p such that $2p + 1$ is also prime.

(2) There are infinitely many primes p such that one of $p + 2, p + 4, \ldots, p + 246$ is also prime.

(3) There is always a prime between n and $2n$ for any integer n.

(4) There is no algorithm which will factor an n-digit integer in at most n^3 steps.

(5) Every non-constant polynomial with complex coefficients has a root (in the complex numbers).

(6) $m \times n = n \times m$ for all integers m and n.

(7) $1 + 1 = 2$.

Remarks

(1) No-one knows if it's true.

(2) Was proved in 2014.

(3) Not obvious but true.

(4) Would be a disaster if false!

(5) The Fundamental Theorem of Algebra.

(6) Worth thinking about...

(7) Does it need proving?

1.2 Some proofs and non-proofs

Assertion. For all positive integers n, $n^3 - n$ is a multiple of 3.

Proof. For any positive integer n, we have

$$n^3 - n = n(n^2 - 1) = n(n+1)(n-1) = (n-1)n(n+1)$$

One of the three consecutive integers $n-1$, n and $n+1$ must be a multiple of 3, and hence, so must their product. □

Notation. The symbol □ is used to mean "end of proof"

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

"Proof". Given a positive integer n, which is even, we can write $n = 2k$ for some positive integer k. Hence $n^2 = (2k)^2 = 2(2k^2)$, which is even. □

Nonsense! We wanted to show "if A then B" but we have shown "if B then A".s

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

This assertion is simply false: take $n = 6$. To guess that "if A then B" is false, then it is enough to show that there is *one* instance where A is true and B is false.

"One counterexample is enough"

Back to: "if n^2 is even, then n is even."
Proof. Suppose on the contrary that n is *not* even. Then n is odd, so $n = 2k+1$ for some integer k. Thus

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

which is odd, contradicting the assumption that n^2 is even. ※ □
This is a proof by contradiction.

Notation (Contradiction)**.** ※ denotes some kind of contradiction in a proof.

To show "if A then B" we shows that there is no case where A is true and B is false. In other words, showing $A \implies B$ is the same as showing NOT $B \implies$ NOT A.

Assertion. The solution to $x^2 - 5x + 6 = 0$ is $x = 2$ or $x = 3$. This is in fact two assertions:

(i) $x = 2$ and $x = 3$ are solutions;

(ii) there are no other solutions.

Proof.

(i) If $x = 2$ or $x = 3$,
then $x - 2 = 0$ or $x - 3 = 0$
so $(x-2)(x-3) = 0$
so $x^2 - 5x + 6 = 0$.

(ii) If $x^2 - 5x + 6 = 0$
then $(x-2)(x-3) = 0$
then $(x-2)(x-3) = 0$
so $x - 2 = 0$ or $x - 3 = 0$
so $x = 2$ or $x = 3$.

□

Or an alternative proof that is more concise:
Proof.

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

□

It is vital that every step is $\iff$!

Assertion. Every positive real is ≥ 1.

"Proof". Let r be the least positive real. Then either $r = 1$ or $r < 1$ or $r > 1$.
If $r > 1$, then $0 < r^2 < r$, contradicting the assumption that r is the least positive real.
If $r > 1$, then $0 < \sqrt{r} < r$, again ⨳ . Hence $r = 1$. □

Nonsense! We don't know that there is a smallest positive real.

Moral. Every claim must be justified.

1.3 Combining Assertions

Notation (Combining assertions)**.** If A and B are assertions, we can (but we usually don't) write $A \wedge B$ for "A AND B", $A \vee B$ for "A OR B", and $\neg A$ for "NOT A".

The truth of these assertions depends on the truth of A and B, summarised in the *truth table*.

A	B	$A \wedge B$
F	F	F
F	T	F
T	F	F
T	T	T

A	B	$A \vee B$
F	F	F
F	T	T
T	F	T
T	T	T

A	$\neg A$
T	F
F	T

A	B	$A \implies B$
F	F	T
F	T	T
T	F	F
T	T	T

Note, for example, that $\neg(A \wedge B)$ is equivalent to $(\neg A) \vee (\neg B)$, by comparing truth tables.
Also, $A \implies B$ is equivalent to $(\neg A) \vee B$ and hence $B \vee (\neg A)$, and hence to $(\neg B) \implies (\neg A)$.

1.4 Qualifiers and Negations

An assertion may involve "quantifiers", for example $\forall n$ ("for all n"), $\exists x$ ("there exists x").

$$\begin{array}{ccc} \neg(\forall x A(x)) & \text{means} & \exists x \neg A(x) \\ \neg(\exists x B(x)) & \text{means} & \forall x \neg B(x) \end{array}$$

The order of quantifiers matters!

2 Elementary Number Theory

Intuitively, the natural numbers consist of

$$1, 1+1, 1+1+1, 1+1+1+1, \ldots$$

How do you know you have captured all natural numbers? How do you know they are all distinct?

2.1 Our Axioms

We shall assume:
The natural numbers, written as $\mathbb{N}$, is a set containing a special element '1' with an operation '+1' satisfying

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

(ii) $\forall m, n \in \mathbb{N}$, if $m \neq n$, then $m + 1 \neq n + 1$;

(iii) for any property $P(n)$, if $P(1)$ is true and $\forall n \in \mathbb{N}$, $P(n) \implies P(n+1)$, then $P(n)$ is true for all natural numbers.

(i) - (iii) are known as the *Peano axioms.*
(iii) is called the *induction axiom.*
(i) & (ii) capture the idea that any two natural numbers are distinct; (iii) captures our intuitive notion that the list is complete (take $P(n) =$ "n is on the list").

Notation. Now we can write 2 for $1 + 1$, 3 for $1 + 1 + 1$, etc, and we can define an operation '+k' for any natural number k in the following way:

$$\text{for every natural number } n, n + (k + 1) = (n + k) + 1.$$

(by induction, taking the statement $P(k) =$ " '+k' is defined"). Similarly, we can define multiplication, powers, etc.

One can check that the "normal" rules of arithmetic apply:

(1) $\forall a, b$ we have $a + b = b + a$ (+ is commutative);

(2) $\forall a, b$ we have $ab = ba$ ($\cdot$ is commutative);

(3) $\forall a, b, c$ we have $a + (b + c) = (a + b) + c$ (+ is associative);

(4) $\forall a, b, c$ we have $a(bc) = (ab)c$ ($\cdot$ is associative);

(5) $\forall a, b, c$ we have $a(b + c) = ab + ac$ (multiplication is distributive over addition).

Definition (Greater than)**.** We define '$a < b$" if $a + c = b$ for some $c \in \mathbb{N}$. One can verify that

(6) $\forall a, b, c \qquad a < b \implies a + c < b + c$;

(7) $\forall a, b, c \qquad a < b \implies ac < bc$;

(8) $\forall a, b, c \qquad a < b \wedge b < c \implies a < c$;

(9) $\forall a \qquad \neg(a < a)$.

Recall the induction axiom: If $P(1)$ holds and $\forall n \in \mathbb{N}$, $P(n) \implies P(n+1)$, then $P(n)$ holds $\forall n \in \mathbb{N}$. This is also known as the *(Weak) Principle of Induction* (WPI). A more useful form is the following.

Definition (Strong Pinciple of Induction (SPI))**.** If

(i) $P(1)$ holds and

(ii) $\forall n \in \mathbb{N}$, we have $P(m) \forall m \leq n \implies P(n+1)$,

then $P(n)$ holds $\forall n \in \mathbb{N}$.

In fact, WPI and SPI are equivalent. To see that WPI implies SPI, apply the former to $Q(n) =$ "$P(m) \forall m \leq n''$.

Theorem (Well-ordering Principle (WOP))**.** If $P(n)$ holds for some $n \in \mathbb{N}$, then there is a least natural number $n \in \mathbb{N}$ such that $P(n)$ holds.

"Every non-empty subset of $\mathbb{N}$ has a minimal element."

Assertion. SPI is equivalent to WOP.

Proof. To show that WOP implies SPI, we assume (i) and (ii), and show that $P(n)$ holds $\forall n \in \mathbb{N}$, using WOP.

Suppose, on the contrary, that $P(n)$ is not true $\forall n \in \mathbb{N}$. Then $C = \{n \in \mathbb{N} : P(n) \text{ is false}\} \neq \emptyset$. By WOP, C has a minimal element, m say. Now $\forall k < m$, $k \notin C$ (by minimality of M), so $P(k)$ holds $\forall k < m$. But by (ii) of SPI, $P(m)$ holds, so contradicting $m \in C$. Hence SPI holds.

To show that SPI implies WOP, suppose there is no least $n \in \mathbb{N}$ such that $P(n)$ holds. We want to show that $P(n)$ does not hold for any $n \in \mathbb{N}$, using SPI.

Consider $Q(n) =$ "$\neg P(n)''$. Certainly $P(1)$ is false (else 1 would be the minimal element), so $Q(1)$ holds.

Given $n \in \mathbb{N}$, suppose that $Q(k)$ is true $\forall k < n$. Then $P(k)$ is false $\forall k < n$. So $P(n)$ is false as otherwise n would be the minimal element for which P holds. Hence $Q(n)$ is true, and so (ii) of SPI holds, so $Q(n)$ is true $\forall n \in \mathbb{N}$. Thus $P(n)$ is false $\forall n \in \mathbb{N}$. □
WOP enables us to prove $P(n)$ is true $\forall n \in \mathbb{N}$ as follows: If not, then there is a minimal counterexample, and we try and derive a contradiction.

2.2 The Integers

The integers, written $\mathbb{Z}$, consist of all symbols

$$n, -n, \text{where } n \text{ is in the natural numbers, and } 0.$$

In other words

$$\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\} \cup \{0\}.$$

Can define $+$ and $\cdot$ etc on $\mathbb{Z}$ from $\mathbb{N}$, and check that the usual rules of arithmetic hold.

We also have the following properties:

(10) $\forall a \in \mathbb{Z} \qquad a + 0 = a$ (identity for $+$)

(11) $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}$ such that $a + b = 0$ (inverses for $+$).

Define "$a < b$" if $a + c = b$ for some $c \in \mathbb{N}$. Then rules (6), (8), (9) continue to hold, but (7) must be modified:

(7') $\forall a, b, c \in \mathbb{Z} \qquad a < b \wedge c > 0 \implies ac < bc.$

2.3 The Rationals

The rationals, written $\mathbb{Q}$, consist of all expressions of the form

$\frac{a}{b}$, where a, b are integers with $b \neq 0$, and $\frac{a}{b}$ and $\frac{c}{d}$ are regarded as the same if $ad = bc$.

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, and one can check that it does not matter how we wrote $\frac{a}{b}$ or $\frac{c}{d}$.

We similarly define multiplication, and define

$$\text{"}\frac{a}{b} < \frac{c}{d}\text{" where } b, d > 0 \text{ if } ad < bc.$$

One can check that rules (6), (7'), (8) and (9) still apply.

In addition:

(12) $\forall a \in \mathbb{Q}, a \neq 0, \exists b$ such that $ab = 1$ (inverses for $\cdot$)

Remark. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

Notation (Subsets)**.** The symbol $\subset$ means "contained in" or "is a subset of".

2.4 Primes

Given $a, b \in \mathbb{Z}$ we say "a divides b"if $\exists c \in \mathbb{Z}$ such that $b = ac$. We might also "a is a divisor of b" or "a is a factor of b", or "b is a multiple of a". We write $a \mid b$.

Remark. For any $b \in \mathbb{Z}$, ± 1 and $\pm b$ are always factors; all other factors (if they exist) are called *proper* or sometimes "non-trivial".

Definition (Primes)**.** A natural number $n \geq 2$ is *prime* if its only factors are ± 1 and $\pm n$.

Definition (Composite numbers)**.** If $n \geq 2$ is not prime, then it is *composite*.

Proposition. Every natural number $n \geq 2$ can be written as a product of primes.

Proof. By induction on n. True for $n = 2$. Let $n > 2$ and suppose that the claim holds up to and including $n-1$. If n is a prime, then done. If n is composite, $n = a \cdot b$ for some $1 < a, b < n$. By the induction hypothesis, we have $a = p_1 \cdots p_k$, $b = q_1 \cdots q_l$ for some primes $p_1 \cdots p_k q \cdots q_l$. Hence $n = ab = p_1 \cdots p_k q_1 \cdots q_l$ is a product of primes. □

Theorem. There are infinitely many primes.

Proof. (Euclid 300BC) Suppose there are finitely many primes, say $p_1, \ldots, p_k$. Let $N = p_1 \cdots p_k + 1$. Then $p_1 \nmid N$, else $p_1 | N - p_1 \cdots p_k = 1$. Note that $\nmid$ means "does not divide". Likewise, none of $p_2, p_3, \ldots, p_k$ divide N, contradicting the fact that N can be written as a product of primes. □ Can a number have more than one factorisation into primes? Our proof that every number has a prime factorisation does not give uniqueness.
Clearly, $21 = 3 \times 7$ is unique.
What about 295869? $= 3 \times 7 \times 73 \times 193$
Why is $9040 \times 40099 \neq 6701 \times 54151$?

We will need the following claim:

Proposition (Euclid's Lemma)**.** If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Definition (Highest Common Factor)**.** Given $a, b \in \mathbb{N}$, a natural number c is the *highest common factor* (hcf), or *greatest common divisor* (gcd) of a and b if

(i) $c \mid a$ and $c \mid b$ ("c is a common divisor of a and b")

(ii) $d \mid a \land d \mid b \implies d \mid c$ "every common factor of a and b divides c"

We write "$c = \text{hcf}(a, b)$" or "$c = \text{gcd}(a, b)$", or simply "$c = (a, b)$".

Example. The factors of 12 are 1, 2, 3, 4, 6, 12 and the factors of 18 are 1, 2, 3, 6, 9, 18. So the common factors are 1, 2, 3, 6, hence $\text{hcf}(12, 18) = 6$. But if a and b had common factors 1, 2, 3, 4, 6, then a and b would have no hcf (according to (ii)). So we need to show that $\text{hcf}(a, b)$ always exists.

Proposition (Division Algorithm)**.** Let $n, k \in \mathbb{N}$. Then we can write $n = qk + r$, where q and r are integers with $0 \le r \le k - 1$.

Proof. By induction on n. True for $n = 1$. Suppose $n - 1 = qk + r$ for some $q, r \in \mathbb{Z}$ such that $0 \le r \le k - 1$. If $r < k - 1$, then $n = (n - 1) + 1 = qk + (r + 1)$. If $r = k - 1$, then $n = (n - 1) + 1 = qk + (k - 1) + 1 = (q + 1)k$. □

Euclid's Algorithm

INPUT	a	b	$a = 372$	$b = 162$
		$q_1 r_1 \in \mathbb{Z}$		
STEP 1	$a = q_1 b + r_1$	$0 \le r_1 \le b - 1$	$372 = 2 \cdot 162 + 48$	
2	$b = q_2 r_1 + r_2$	$0 \le r_2 < r_1$	$162 = 3 \cdot 48 + 18$	
3	$r_1 = q_3 \cdot r_2 + r_3$	$0 \le r_3 < r_2$	$48 = 2 \cdot 18 + 12$	
	$\vdots$			
n	$r_{n-2} = q_n r_{n-1} + r_n$	$0 \le r_n < r_{n-1}$	$18 = 1 \cdot 12 + 6$	
$n + 1$	$r_{n-1} = r_{n=1} r_n + r_{n+1}$	$= 0$	$12 = 2 \cdot 6$	
OUTPUT	r_n		6	

Note that the algorithm terminates in $\le b$ steps, since $b > r_1 > r_2 > \cdots \ge 0$.

Theorem. The output of Euclid's algorithm with input a, b is $\text{hcf}(a, b)$.

Proof.

(i) Have $r_n \mid r_{n-1}$ (as $r_{n+1} = 0$ at STEP $n + 1$)
so $r_n \mid r_{n-2}$ (STEP n)

so $r_n \mid r_i \;\; \forall i = 1, \dots, n-1$ (by induction)
Hence $r_n \mid b$ (STEP 2) and $r_n \mid a$ (STEP 1).

(ii) Given d such that $d \mid a$ and $d \mid b$,
have $d \mid r_1$ (STEP 1)
so $d \mid r_2$ (STEP 2)
and $d \mid r_i \forall i = 1, \dots, n$ by induction.

□

Definition (Coprime)**.** When $\text{hcf}(a, b) = 1$, we also say that a and b are *coprime.*

Example ($\text{hcf}(87, 52)$)**.**

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

so $\text{hcf}(87, 52) = 1$.
We can also reverse the algorithm:

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

Theorem. For all natural numbers a and b, there exists some integers x and y such that

$$xa + yb = \text{hcf}(a, b)$$

"We can write $\text{hcf}(a, b)$ as a linear combination of a and b."

Proof 1. Run Euclid's algorithm with input a, b to obtain an output r_n say. At STEP n, have $r_n = xr_{n-1} + yr_{n-2}$ for some $x, y \in \mathbb{Z}$. But r_{n-1} is expressible as $xr_{n-2} + yr_{n-3}$ for some $x, y \in \mathbb{Z}$, from STEP $n-1$, whence $r_n = xr_{n-2} + yr_{n-3}$ for some $x, y \in \mathbb{Z}$. Continuing by induction, we have $\forall i = 2, \dots, n-1$, $r_n = xr_i + yr_{i-1}$ for some $x, y \in \mathbb{Z}$. Thus $r_n = xa + yb$ for some $x, y \in \mathbb{Z}$, from STEP 1 and 2. □

Remark. Euclid's algorithm not only proves that $x, y \in \mathbb{Z}$ exist, but it gives us a quick way to find them.

Proof 2. Let h be the least positive linear combination of a and b, i.e. the least positive integer of the form $xa + yb$ for some $x, y \in \mathbb{Z}$.
We will show that $h = \text{hcf}(a, b)$.
To see that part (ii) of the definition of hcf holds, observe that given d such that $d \mid a$ and $d \mid b$, then we have that $d \mid ax + by \ \forall x, y \in \mathbb{Z}$, so in particular, $d \mid h$.
To verify part (i), suppose that $h \nmid a$. Then we can write $a = qh + r$ for some $q, r \in \mathbb{Z}$ with $0 < r < h$ (note that the strict inequality on the 0 comes from the fact that we have assumed that $h \nmid a$). Hence $r = a - qh = a - q(xa + yb)$ is also a positive linear combination of a and b, and strictly smaller than h contradicting the definition of h. Therefore $h \mid a$, and by the same argument $h \mid b$.
Therefore $h = \text{hcf}(a, b)$. □

Remark. Proof 2 also tells us that the $\text{hcf}(a, b)$ exists and is a linear combination of a and b, *but* gives no way to find $\text{hcf}(a, b)$ or the coefficients x, y.

Is there a solution in integers x, y to the equation

$$320x + 72y = 33?$$

No, as LHS always even and the RHS odd.
What about $87x + 52y = 33$? Yes, as we had $x', y' \in \mathbb{Z}$ such that $87x' + 52y' = 1$, so $x = 33x'$, $y = 33y'$ is an integer solution.

Corollary 1 (Bézout's Theorem)**.** Let $a, b \in \mathbb{N}$. Then the equation $ax + by = c$ has a solution in integers x, y if and only if $\text{hcf}(a, b) \mid c$.

Proof. Let $h = \text{hcf}(a, b)$.
To prove that "only if" direction, suppose there are $x, y \in \mathbb{Z}$ such that $ax + by = c$. Then since $h \mid a$ and $h \mid b$, then $h \mid c$.
Conversely, suppose $h \mid c$. But this implies that there exist $x, y \in \mathbb{Z}$ such that $h = ax+by$. But then

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

□

Now we will prove Euclid's Lemma, which was stated earlier.

Proposition (Euclid's Lemma)**.** If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Suppose $p \mid ab$ but $p \nmid a$. We will show that $p \mid b$. Since p is prime, $\operatorname{hcf}(a,p)$ must be either 1 or p, but since $p \nmid a$ it cannot be p, hence we must have that $\operatorname{hcf}(a,p) = 1$. Thus there exist $x, y \in \mathbb{Z}$ such that $xp + ya = 1$.
It follows that $xpb + yab = b$ hence b is a multiple of p (as each of p and ab is). □

Remarks

(1) Similarly, $p \mid a_1 a_2 \cdots a_n \implies p \mid a_i$ for some $i = 1, \ldots, n$. Indeed, the proposition tells us that if $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_1$ or $p \mid a_2 \cdots a_n$. Proceed by induction on the number of terms in the product.

(2) We do need p prime.

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

Proof. We have already proved existence of a factorisation, so we need only prove that it is unique. To prove this, we use induction on n. It is clearly true for $n = 2$. Given $n \geq 2$, suppose $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, where p_i, q_j are all prime. We want to show that $k = l$, and after reordering $p_i = q_i$ $\forall i = 1, \ldots, k$. We have that $p_1 \mid n$, hence $p \mid q_1 \cdots q_l$, so p_1 must divide one of the factors in this product, so $p_1 \mid q_i$ for some i. Relabelling the q_i, we may assume that $p_1 \mid q_1$. Since q_1 is prime, we must have $p_1 = q_1$, so $\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l < n$. By the induction hypothesis, $k = l$, and after reordering, $p_2 = q_2$, …, $p_k = q_k$, so the factorisations were the same. □

Remark. There are "arithmetical systems" (permitting addition, subtraction, multiplication) where factorisation is *not* unique.
For example, consider $\mathbb{Z}[\sqrt{-3}]$, meaning all complex numbers of the form $x + y\sqrt{-3} = x + y\sqrt{3}i$, where $x, y \in \mathbb{Z}$. We can add, subtract and multiply two elements of $\mathbb{Z}[\sqrt{-3}]$ to get another element of $\mathbb{Z}[\sqrt{-3}]$. For example

$$(1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}) = 1 + \sqrt{-3} - \sqrt{-3} - (\sqrt{-3})^2 = 1 + 3 = 4.$$

In $\mathbb{Z}[\sqrt{-3}]$ we can define what it means to be a "prime", and both $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ happen to be primes in this sense. But we can also write $4 = 2 \cdot 2$, so factorisation is not unique.

2.5 Some Applications of the Fundamental Theorem of Arithmetic

(i) What are the factors of $n = 2^3 \cdot 3^7 \cdot 11$? All numbers of the form $2^a \cdot 3^b \cdot 11^c$, where $0 \leq a \leq 3$, $0 \leq b \leq 7$ and $0 \leq c \leq 1$ are factors. There are no other others: if for example, $7 \mid n$, then we would have a factorisation of n involving 7, contradicting uniqueness. More generally, the factors of $n = p_1^{a_1} \cdots p_k^{a_k}$ are precisely the numbers of the form $p_1^{b_1} \cdots p_k^{b_k}$, with $0 \leq b_i \leq a_i$ $\forall i = 1, \ldots, k$.

(ii) What are the common factors of

$$2^3 \cdot 3^7 \cdot 5 \cdot 11^3 \qquad \text{and} \qquad 2^4 \cdot 3^2 \cdot 11 \cdot 13?$$

All numbers of the form $2^a \cdot 3^b \cdot 5^c \cdot 11^d \cdot 13^e$, where $e = c = 0$ and $0 \leq a \leq 3$, $0 \leq b \leq 2$ and $0 \leq d \leq 1$. Thus the hcf is $2^3 \cdot 3^2 \cdot 11$. In general, the hcf of $p_1^{a_1} \cdots p_k^{a_k}$ and $p_1^{b_1} \cdots p_k^{b_k}$, where $a_i, b_i \geq 0$, is $p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}$.

(iii) What are the common multiples of the two numbers in the previous example? All numbers of the form $a2^a \cdot 3^b \cdot 5^c \cdot 11^d \cdot 13^e$, where $a \geq 4$, $b \geq 7$, $c \geq 1$, $d \geq 3$, $e \geq 1$, *times* any integer! Hence $2^4 \cdot 3^7 \cdot 5 \cdot 11^3 \cdot 13$ is a common multiple, and any other common multiple is a multiple of it. We say that it is the *least common multiple* (lcm) of our two numbers. In general, the lcm of $p_1^{a_1} \cdots p_k^{a_k}$ and $p_1^{b_1} \cdots p_k^{b_k}$, with $a_i, b_i \geq 0$, is $p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}$. Since

$$\min\{a_i, b_i\} + \max\{a_i, b_i\} = a_i + b_i,$$

we have

$$\mathrm{hcf}(x, y) \cdot \mathrm{lcm}(x, y) = x \cdot y,$$

for any x, y.

(iv) Another proof of the infinitude of primes, due to Erdős (1930):
Let $p_1, \ldots, p_k$ be primes. Any number which is a product of just these primes is of the form $(*) = p_1^{j_1} \cdot p_2^{j_2} \cdots p_k^{j_k} = m^2 \cdot p_1^{i_1} \cdot p_2^{i_2} \cdots p_k^{i_k}$ where $i_k = 0, 1$. Let $M \in \mathbb{N}$. If a number $\leq M$ is of the form $(*)$, then $m^2 \leq M$, i.e. $m \leq \sqrt{M}$. So there are at most $\sqrt{M} \cdot 2^k$ numbers of the form $(*)$ that are $\leq M$.
If $M > \sqrt{M} \cdot 2^k$, i.e. $M > 4^k$, then there must be a number $\leq M$ which is *not* of the form $(*)$, which must have a prime factor not amongst the $p_1, \ldots, p_k$ (because otherwise we could write it in the form $(*)$). The first proof we saw of the infinitude of primes told us that the k-th prime is $< 2^{2^k}$. This proof by Erdős tells us that the k-th prime is $< 4^k$. In fact, we know that the k-th prime is $\sim k \log k$, by the Prime Number Theorem.

2.6 Modular Arithmetic

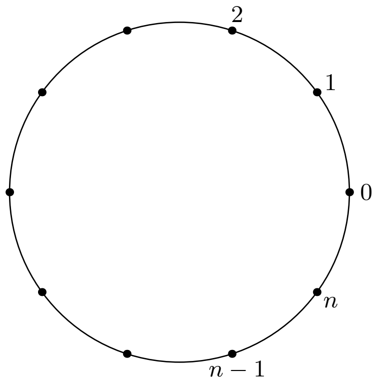
Let $n \geq 2$ be a natural number. Then the *integers modulo* n, written $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, consist of the integers, with two regarded as the same if they differ by a multiple of n. For example, in $\mathbb{Z}_7$, 2 is the same as 16. If x and y are the same in $\mathbb{Z}_n$, we write

$$x \equiv y \pmod{n} \qquad \text{or} \qquad x \equiv y(n) \qquad \text{or} \qquad x = y \text{ in } \mathbb{Z}_n$$

The first two are read as “x is equivalent to y modulo n” and the last one is read in the obvious way. For example $2 \equiv 16 \pmod{7}$. Thus

$$\begin{aligned} x \equiv y \pmod{n} &\iff n \mid x - y \\ &\iff x = y + kn \qquad \text{for some } k \in \mathbb{Z} \end{aligned}$$

Similarly to visualising the natural numbers using the number line, we can view $\mathbb{Z}_n$ as a circle:



Remark. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$n \mid (a-a') + (b-b') = (a+b) - (a'+b') \implies a+b \equiv a'+b' \pmod{n}$$

Similarly,

$$n \mid (a-a') \cdot b + a' \cdot (b-b') = ab - a'b' \implies ab = a'b' \pmod{n}.$$

So we can *arithmetic* modulo n.

Example. Does $2a^2 + 3b^3 = 1$ have a solution with $a, b \in \mathbb{Z}$?

Answer. There are no solutions

Proof. If there is a solution, then $2a^2 \equiv 1 \pmod{3}$, but $2 \cdot 0^2 \equiv 0$ $2 \cdot 1^2 \equiv 1$, $2 \cdot 2^2 \equiv 2 \pmod{3}$. □

2.7 Solving Congruences

Example. Solve $7x \equiv 2 \pmod{10}$.
We note that $3 \cdot 7 \equiv 1 \pmod{10}$, so $3 \cdot 7x \equiv 3 \cdot 2 \pmod{10}$ hence $x \equiv 6 \pmod{10}$.

Given $a, b \in \mathbb{Z}$, we say that b is an *inverse of a modulo n* if $ab \equiv 1 \pmod{n}$. We say a is *invertible modulo n*, or is a *unit modulo n*, if it has inverse.
For example, in $\mathbb{Z}_{10}$, the inverse of 3 is 7 and both 3 and 7 are units modulo 10.
On the other hand, 4 is *not* a unit modulo 10 since $4x \not\equiv 1 \pmod{10}$ $\forall z \in \mathbb{Z}$.

Remarks

If a is a unit modulo n then…

(1) Its inverse is unique. Proof: suppose $\exists b, b'$ such that $ab \equiv ab' \equiv 1 \pmod{n}$, then $b \equiv bab \equiv bab' \equiv b' \pmod{n}$.

(2) We can write a^{-1} for its inverse.

(3) And $ab \equiv ac \pmod{n}$ always implies that $b \equiv c \pmod{n}$ "We cancel units, multiplying both sides by a^{-1}." This is *not* true in general: $4 \cdot 3 \equiv 4 \cdot 8 \pmod{10}$ but $3 \not\equiv 8 \pmod{10}$.

Proposition. Let p be prime. Then every $a \not\equiv 0 \pmod{p}$ is a unit modulo p.

Proof. Have $(a, p) = 1$, so $\exists x, y \in \mathbb{Z}$ such that $ax + py = 1$. Hence $ax = 1 - py$, so $ax \equiv 1 \pmod{p}$ for some $x \in \mathbb{Z}$. □

Proposition. Let $n \geq 2$. Then a is a unit modulo n if and only if $(a, n) = 1$.

Proof.

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

□

Corollary 2. If $(a, n) = 1$, then the congruence $ax \equiv b \pmod{n}$ has a unique solution. In particular, if $(a, n) = 1$, then there is a unique inverse of a, a^{-1} modulo n.

What if $ax \equiv b \pmod{n}$ with $(a, n) \neq 1$, say $(a, n) = d > 1$?
Then $n \mid ax - b$ so $d \mid ax - b$ and $d \mid a$, so if there is a solution, then $d \mid b$.
Conversely, if $d \mid b$, then $n = d \cdot n'$, $a = d \cdot a'$, $b = d \cdot b'$, and

$$\begin{aligned} ax \equiv b \pmod{n} &\iff ax - b = kn \qquad \text{for some } k \in \mathbb{Z} \\ &\iff d \cdot a' \cdot x - d \cdot b' = k \cdot d \cdot n' \\ &\iff a'x - b' = kn' \\ &\iff a'x \equiv b' \pmod{n'}. \end{aligned}$$

Note $(a', n') = 1$.
So if $(a, n) = d > 1$, the congruence $ax \equiv b \pmod{n}$ has no solution unless $d \mid b$, in which case the solutions are exactly those of $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Examples

(1) Solve $7x \equiv 4(30)$.
We have $(7, 30) = 1$, so by Euclid $13 \cdot 7 - 3 \cdot 30 = 1$. Hence $13 \cdot 7 \equiv 1 \pmod{30}$, whence $x \equiv 4 \cdot 13 \equiv 22 \pmod{30}$.
Suppose x' is also a solution, that is, $7x' \equiv 4 \pmod{30}$. Then $7x \equiv 7x' \pmod{30}$, so $x \equiv x' \pmod{30}$ since 7 is a unit modulo 30.
Short form:

$$\begin{aligned} & 7x \equiv 4 \pmod{30} \\ \iff & 13 \cdot 7x \equiv 13 \cdot 4 \pmod{30} \\ \iff & x \equiv 22 \pmod{30}. \end{aligned}$$

(2) Solve $10x \equiv 12 \pmod{34}$.

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

so now we're back in situation (1), and solve as before.

2.8 Solving Simultaneous Congruences

Note

$$x \equiv 5 \pmod{12} \implies \begin{cases} x \equiv 1 & \pmod 4 \\ x \equiv 2 & \pmod 3 \end{cases}$$

Is the converse true, i.e. does $x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$ imply $x \equiv 5 \pmod{12}$? We inspect:

$$\begin{aligned} x \equiv 1 \pmod 4 \qquad & x \equiv 1 \;\; 5 \;\; 9 \pmod{12} \\ x \equiv 2 \pmod 3 \qquad & x \equiv 2 \;\; 5 \;\; 8 \;\; 11 \pmod{12} \end{aligned}$$

Note that 5 is a common solution.
What about

$$\begin{cases} x \equiv 1 & \pmod 4 \\ x \equiv 2 & \pmod 6 \end{cases}?$$

Theorem ((12) The Chinese Remainder Theorem)**.** Let m, n be coprime, and $a, b \in \mathbb{Z}$. Then there is a unique solution modulo mn to the simultaneous congruences

$$x \equiv a \pmod m \qquad \text{and} \qquad x \equiv b \pmod n.$$

That is, there is a solution x to $x \equiv a \pmod m$ and $x \equiv b \pmod n$, and y is a solution if and only if $x \equiv y \pmod{mn}$.

Proof. Existence: Since $(m, n) = 1$, $\exists s, t \in \mathbb{Z}$ with $sm + tn = 1$. Note

$$\begin{aligned} sm &\equiv t \pmod{n} \qquad \text{and} \qquad & tn &\equiv 1 \pmod{m} \\ sm &\equiv 0 \pmod{m} & tn &\equiv 0 \pmod{n}. \end{aligned}$$

Hence $x = a(tn) + b(sm) \equiv a \pmod{m}$ and $x = a(tn) + b(sm) \equiv b \pmod{n}$.
Uniqueness: Suppose y is also a solution, that is,

$$\begin{aligned} & y \equiv a \pmod{m} \qquad \text{and} \qquad y \equiv b \pmod{n} \\ \iff & y \equiv x \pmod{m} \qquad \text{and} \qquad y \equiv x \pmod{n} \\ \iff & m \mid y - x \qquad \text{and} \qquad n \mid y - x \\ \iff & mn \mid y - x \qquad \text{since } (m, n) = 1 \\ \iff & y \equiv x \pmod{mn} \end{aligned}$$

□

Remark. Theorem 12 can be extended, by induction, to more than two moduli: if $m_1, m_2, \ldots, m_k$ are pairwise coprime, then $\forall a_1, a_2, \ldots, a_k \in \mathbb{Z}$,

$$\begin{aligned} \exists x \in \mathbb{Z} \text{ such that } x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

We denote by $\varphi(m)$ the number of integers a such that $1 \le a \le m$ and $(a, m) = 1$, that is, the number of units modulo n. We call φ the *Euler totient function.* Define $\varphi(1) = 1$. For example when p is prime, $\varphi(p) = p - 1$, and $\varphi(p^2) = p^2 - p$. When p, q are distinct primes,

$$\varphi(pq) = pq - p - q + 1.$$

How do powers of an integer behave modulo p?

Example. Modulo 7, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, $2^4 \equiv 2$ then repeat $4, 1, 2, 4, 1, 2, \ldots$.
Modulo 11 $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 1$, then repeats.

Theorem ((13) Fermat's Little Theorem)**.** Let p be prime. Then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Equivalently, $a^{p-1} \equiv 1 \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$.

Proof. If $a \not\equiv 0 \pmod{p}$, then a is a unit modulo p. Thus $ax \equiv ay \pmod{p}$ if and only if $x \equiv y \pmod{p}$. Hence the numbers $a, 2a, 3a, \dots, (p-1)a$ are pairwise incongruent (distinct) modulo p and $\not\equiv 0 \pmod{p}$, so they are $1, 2, 3, \dots, p-1$ in some order. Hence

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

so

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

But $(p-1)!$ is a unit modulo p (since it is a product of units), so we can cancel it to obtain

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

□

Theorem (Fermat-Euler Theorem)**.** Let $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof. Let $U = \{x \in \mathbb{N} : 0 < x < m : (x, m) = 1\}$ be the set of units modulo m. Label the elements $u_1, u_2, \dots, u_{\varphi(m)}$. Then $au_1, au_2, \dots, au_{\varphi(m)}$ are all distinct and invertible modulo m (since a is a unit), and hence they are $u_1, u_2, \dots, u_{\varphi(m)}$, in some order.
It follows that

$$au_1 \cdot au_2 \cdots au_{\varphi(m)} \equiv u_1 \cdot u_2 \cdots u_{\varphi(m)} \pmod{m}$$

that is

$$a^{\varphi(m)} z = z \pmod{m}$$

where $z = u_1 u_2 \cdots u_{\varphi(m)}$ is a product of units modulo m, whence itself is a unit. We may cancel it to obtain $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

What is $(p-1)!$ modulo p?

Example. When $p = 5$, $4! = 24 \equiv -1 \pmod{5}$ and when $p = 7$, $6! = 720 \equiv -1 \pmod{7}$.

Lemma 1 (14)**.** Let p be a prime. Then $x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$.

Remark. Modulo 8, $1^2 = 3^2 = 5^2 = 7^2 = 1$, so this lemma is not true in general.

Proof.

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff x^2 - 1 \equiv 0 \pmod{p} \\ &\iff (x+1)(x-1) \equiv 0 \pmod{p} \end{aligned}$$

Recall Euclid's Lemma: if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$, so if p is prime, then $ab \equiv 0 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.
Hence

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff x + 1 \equiv \quad \pmod{p} \qquad \text{or} \qquad x - 1 \equiv 0 \pmod{p} \\ &\iff x \equiv -1 \pmod{p} \qquad \text{or} \qquad x \equiv 1 \pmod{p} \end{aligned}$$

□

Remark. More generally, a non-zero polynomial of degree k over $\mathbb{Z}_p$ has at most k roots in $\mathbb{Z}_p$.

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

Proof. True for $p = 2$, so assume $p > 2$.
Note that the units modulo p come in pairs whose product is 1, together with some elements that are self inverse, i.e. x such that $x \cdot x \equiv 1 \pmod{p}$. But by Lemma 14, the elements of $\mathbb{Z}_p$ that are self-inverse are $+1$ and -1, so the remaining $p - 3$ elements of $\mathbb{Z}_p$ come in inverse pairs.
For example when $p = 11$ the pairs are $(1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (10, 10)$.
Hence $(p-1)!$ is the product of $\frac{p-3}{2}$ pairs of inverses together with $+1$ and -1, so $(p-1)! \equiv -1 \pmod{p}$. □

When is -1 a square modulo p? (If ever.)

Example. When $p = 5$, $2^2 \equiv 4 \equiv -1 \pmod{5}$. When $p = 7$, $0^2 = 0$, $1^1 = 1$, $2^2 = 4$, $3^2 = 2$ modulo 7, and we don't need to check 4, 5, 6 as $(-x)^2 = x^2$. So -1 is not a square number modulo 7. When $p = 13$, $5^2 \equiv -1 \pmod{13}$. No luck when $p = 19$.

Proposition (16)**.** Let p be an odd prime. Then -1 is a square modulo p if and only if $p \equiv 1 \pmod{4}$.

Proof. Suppose $p \equiv 1 \pmod{4}$. By Wilson's Theorem,

$$\begin{aligned} -1 &\equiv (p-1)! && \pmod{p} \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \cdots (-3)(-2)(-1) && \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 && \pmod{p} \end{aligned}$$

But if $p = 4k + 1$ for some $k \in \mathbb{Z}$, then

$$-1 \equiv (-1)^{2k}((2k)!)^2 \pmod{p},$$

so -1 is a square modulo p.
Suppose, on the other hand, that $p \equiv -1 \pmod{4}$, i.e. $p = 4k + 3$ for some $k \in \mathbb{Z}$.
If -1 were a square modulo P, i.e. if there were $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \pmod{p}$, then by Fermat's Little Theorem,

$$1 \equiv z^{p-1} \equiv z^{4k+2} \equiv z^{2(2k+1)} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$$

a contradiction. □

Remark. When $p \equiv 1 \pmod{4}$, Wilson's Theorem tells us a solution to the equation $x^2 \equiv -1 \pmod{p}$. For example, when $p = 29 = 4 \cdot 7 + 1$, $x = (2 \cdot 7)!$ works.

2.9 Public Key Cryptography

Let us agree to write messages as sequences of numbers, for example $A \to 00$, $B \to 01$, $\ldots$, $Z \to 25$, $! \to 26$, etc.
I wish for my IA students to be able to send me messages in encrypted form in such a way that I can decrypt them easily but the same is not true of any third-party observer.
We use the RSA Scheme.

RSA Scheme (Rivest, Shamir, Adlemann)

I think of two large primes p, q. Let $n = pq$, and pick an *encoding exponent* e coprime to $\phi(n) = (p-1)(q-1)$.
I publish the pair (n, e).
To send me a message (i.e. a sequence of numbers) you chop it into pieces / numbers $M < n$ and send me $M^e \pmod{n}$, computed quickly by repeated squaring (binary exponentiation).

To decrypt, I work out d such that $ed \equiv 1 \pmod{\phi(n)}$, i.e. some d such that $ed = k\phi(n) + 1$ for some $k \in \mathbb{Z}$. Then I compute

$$(M^e)^d \equiv M^{k\phi(n)+1} \equiv M \pmod{n}$$

by Fermat-Euler.

Note that in order to decrypt in this way, needed n and d, or n, e and $\phi(n)$. Finding $\phi(n)$ is as hard as finding the prime factors of n, which is believed to be computationally hard.
It is not known if RSA can be broken without factorisation.

CHAPTER III: The Reals

1 Motivation

We had seen $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.
Why not stop here?

Proposition 1. There is no rational x with $x^2 = 2$.

Proof 1. Suppose $x^2 = 2$. Note we can assume $x > 0$ since $(-x)^2 = x^2$. If x is rational and position, then $x = \frac{a}{b}$ for some $a, b \in \mathbb{N}$. Thus $\frac{a^2}{b^2} = 2$, or $a^2 = 2b^2$. But the exponent of 2 in the prime factorisation of a^2 is even while the exponent of 2 in the prime factorisation of $2b^2$ is odd, contradicting the Fundamental Theorem of Arithmetic. □

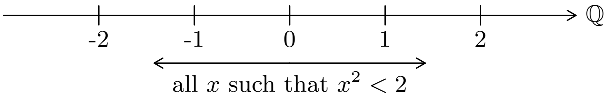
Note. The same proof shows that if $\exists x \in \mathbb{Q}$ with $x^2 = n$ for some $n \in \mathbb{N}$, then n must be a square.

Proof 2. Suppose $x^2 = 2$ for some $x = \frac{a}{b}$ with $a, b \in \mathbb{N}$. Then for any $c, d \in \mathbb{Z}$, $cx + d$ is of the form $\frac{e}{b}$ for some $e \in \mathbb{Z}$. Thus if $cx + d > 0$, then $cx + d \geq \frac{1}{b}$. But $0 < x - 1 < 1$ as $1 < x < 2$ so if n is sufficiently large,

$$0 < (x-1)^n < \frac{1}{b}$$

But for any $n \in \mathbb{N}$, $(x-1)^n$ is of the form $cx+d$ for some $c, d \in \mathbb{Z}$, since we can binomially expand and use $x^2 = 2$. This is a contradiction. □

So "$\mathbb{Q}$ has a gap".
How do we express this fact making reference only to $\mathbb{Q}$?



2 is an upper bound for the set of x such that $x^2 < 2$, but so is 1.5, and 1.42, ...

Crucial point. In $\mathbb{Q}$, there is no least upper bound.

2 Reals

The real numbers, written $\mathbb{R}$ are a set with elements 0 and 1 ($0 \neq 1$), equipped with operations $+$ and $\cdot$, and an ordering $<$ such that

(1) $+$ is commutative and associative with identity 0, and every x has an inverse under $+$;

(2) $\cdot$ is commutative and associative with identity 1, and every $x \neq 0$ has an inverse under $\cdot$;

(3) $\cdot$ distributive over $+$, that is, for all $a, b, c \in \mathbb{R}$

$$a(b+c) = ab + ac;$$

(4) $\forall a, b$, exactly one of $a < b$ or $a = b$ or $a > b$ holds, and $\forall a, b, c$,

$$a < b \text{ and } b < c \implies a < c;$$

(5) $\forall a, b, c$, $a < b \implies a + c < b + c$ and $a < b \implies ac < bc$ if $c > 0$.

(6) Given any set S of reals that is non-empty and bounded above, S has a least upper bound. (This is known as the *least upper bound axiom.*)

We say that a set S is *bounded above* if $\exists x \in \mathbb{R}$ such that $x \geq y \ \forall y \in S$. Such an x is called an *upper bound for S*. x is the *least upper bound for S* if x is an upper bound for S and every other upper bound x' satisfies $x' \geq x$.
When x is a least upper bound for S, we may write "LUB(S) $= x$" or "supremum(S) $= x$" or "sup(S) $= x$".

Remarks

(i) From (1)-(5), we can check, for example, that $0 < 1$. Indeed, if not, then $1 < 0$ ($0 \neq 1$) so

$$0 = 1 - 1 < 0 - 1 = -1$$

so

$$0 = 0 \cdot (-1) < (-1)(-1) = 1,$$

a contradiction.

(ii) We may consider $\mathbb{Q}$ as contained in $\mathbb{R}$, by identity $\frac{a}{b} \in \mathbb{Q}$ with $a \cdot b^{-1} \in \mathbb{R}$.

(iii) $\mathbb{Q}$ does not satisfy (6), for example the set of x such that $x^2 < 2$ does not have a supremum.

(iv) In (6), the words "non-empty" and "bounded above" are crucial:

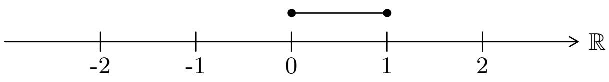
- If S is empty then every $x \in \mathbb{R}$ is an upper bound for S, so there is no least upper bound.

- If S is not bounded above, then it has no upper bound, and certainly no *least* upper bound.

(v) It is possible to construct $\mathbb{R}$ "out of" $\mathbb{Q}$ and check (1)-(6) hold, but it takes a lot of effort.

Examples

(1) $S = \{x \in \mathbb{R} : 0 \leq x \leq 1\} = [0, 1]$ ("the set of $x \in \mathbb{R}$ such that $0 \leq x \leq 1$")

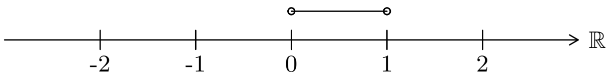


Is 2 an upper bound for S? Yes: $\forall x \in S$, $x \leq 2$.
Is $\frac{3}{4}$ an upper bound for S? No: $\frac{7}{8} \in S$ and $\frac{7}{8} > \frac{3}{4}$.
The least upper bound of S is 1 because

- 1 is an upper bound (as $\forall x \in S$, $x \leq 1$)
- every other upper bound y has $y \geq 1$ (as $1 \in S$).

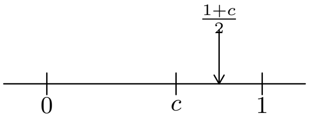
Hence $\sup(S) = 1$.

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



Is 2 an upper bound for S? Yes: $\forall x \in S$, $x \leq 2$.
Is $\frac{3}{4}$ an upper bound for S? No: $\frac{7}{8} \in S$ and $\frac{7}{8} > \frac{3}{4}$.
We have $\sup(S) = 1$ because

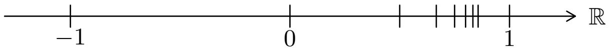
- 1 is an upper bound (as $\forall x \in S$, $x \leq 1$);
- no upper bound c is such that $c < 1$. Indeed, c is certainly greater than 0 (in fact $c \geq \frac{1}{2}$ since $\frac{1}{2} \in S$), so if $c < 1$, then $0 < c < 1$, so $\frac{c+1}{2} \in S$ with $\frac{1+c}{2} > c$.



Hence $\sup(S) = 1$.

> **Remark.** If S has a greatest element, then $\sup(S) = \max(S) \in S$. But $\sup(S)$ can exist when $\max(S)$ does not, in which case $\sup(S) \notin S$.

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

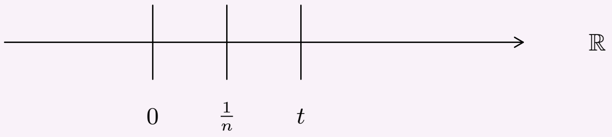


Clearly 1 is an upper bound. Is there an upper bound < 1?

Proposition 2 (Axiom of Archimedes)**.** $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Proof. Suppose on the contrary that $\mathbb{N}$ is bounded above. Let $c = \sup(\mathbb{N})$. By definition $c - 1$ is no an upper bound for $\mathbb{N}$, so $\exists n \in \mathbb{N}$ such that $n > c - 1$. But then $n + 1 \in \mathbb{N}$ with $n + 1 > c$, contradicting the fact that c was an upper bound. □

Corollary 3. For all $t > 0$, $\exists n \in \mathbb{N}$ with $\frac{1}{n} < t$.

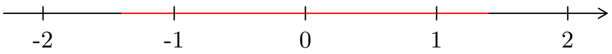


Proof. Given $t > 0$, by Proposition 2, $\exists n \in \mathbb{N}$ such that $n > \frac{1}{t}$. Hence $\frac{1}{n} < t$. □ A set S is said to be *bounded below* if $\exists x$ such that $x \leq y$ $\forall y \in S$. Such an x is called a *lower bound for S*. If S is non-empty and bounded below, then $-S = \{-y : y \in S\}$ is non-empty and bounded below, then $-S = \{-y : y \in S\}$ is non-empty and bounded above, so it has a least upper bound, c say. Hence $-c$ is the *greatest lower bound of S*. We denote it by "GLB(S)", or "infimum(S)" or "inf(S)".
Corollary 3 immediately implies that $\inf(\{\frac{1}{n} : n \in \mathbb{N}\}) = 0$.
Proposition 2 and Corollary 3 show that there are no "infinitely large" or "infinitely small" numbers in $\mathbb{R}$.

Back to Example (3): we have $\sup(S) = 1$, for suppose $c < 1$ is an upper bound for S. Then $1 - \frac{1}{n} < c$ $\forall n \in \mathbb{N}$, so $0 < 1 - c < \frac{1}{n}$ $\forall n \in \mathbb{N}$ contradicting Corollary 3.

Theorem (4)**.** There exists $x \in \mathbb{R}$ with $x^2 = 2$.

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



Note that S is non-empty since for example $1 \in S$. It is also bounded above, for example by 2. Hence S has a supremum, which we denote by c, say.
Observe that $1 < c < 2$. We claim that $c^2 = 2$. Suppose on the contrary that $c^2 < 2$. For $0 < t < 1$, have

$$\begin{aligned}(c+t)^2 &= c^2 + 2ct + t^2 \\ &< c^2 + 5t \\ &< 2\end{aligned}$$

for small t (namely, $t < \frac{2-c^2}{5}$). But this contradicts the assumption that c was an upper bound for S (since $c + t \in S$). Suppose now that $c^2 > 2$. For $0 < t < 1$, have

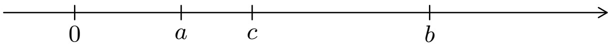
$$\begin{aligned}(c-t)^2 &= c^2 - 3ct + t^2 \\ &\geq c^2 - 4t \\ &> 2\end{aligned}$$

for small t (namely, $t < \frac{c^2-2}{4}$). This contradicts the assumption that c is the *least* upper bound for S (since $c - t$ is an upper bound for S). □

Remark. The same proof shows that $\sqrt[n]{x}$ exists $\forall n \in \mathbb{N}$, $\forall x \in \mathbb{R}$, $x > 0$. (i.e. $\forall n \in \mathbb{N}$, $\forall x \in \mathbb{R}$, $x > 0$; $\exists y \in \mathbb{R}$ such that $y^n = x$.)

A real that is not rational is called *irrational*. For example, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$ are irrational. Also, $2 + 3\sqrt{5}$ is irrational. Indeed, if $2 + 3\sqrt{5} = \frac{a}{b}$ with $a, b \in \mathbb{N}$, then $\sqrt{5} = \frac{a-2b}{3b} \in \mathbb{Q}$, ⨳. □

The rationals are *dense* in $\mathbb{R}$, in the sense that $\forall a < b \in \mathbb{R}$, $\exists c \in \mathbb{Q}$ with $a < c < b$.



Indeed, we may assume that $a \geq 0$. By corollary 3, $\exists n \in \mathbb{N}$ with $\frac{1}{n} < b - a$. By the Axiom of Archimedes, $\exists N \in \mathbb{N}$ such that $N > b$. Let $T = \{k \in \mathbb{N} : \frac{k}{n} \geq b\}$, then $Nn \in T$, so $T \neq \emptyset$. By the Well-Ordering Principle, T has a least element m. Set $c = (m-1) \cdot \frac{1}{n}$. Since $m - 1 \notin T$, $c < b$. If $c \leq a$, then $\frac{m}{n} = c + \frac{1}{n} < a + b - a = b$. ⨳ Hence $a < c < b$. □

Notation. $\emptyset$ denotes the empty set.

Notation. For some sets S_1 and S_2, $S_1 \setminus S_2$ denotes the set of elements in S_1 but not S_2.

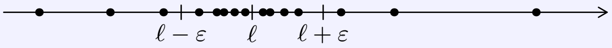
The irrationals are also dense in $\mathbb{R}$, i.e. $\forall a < b \in \mathbb{R}$, $\exists c \in \mathbb{R} \setminus \mathbb{Q}$ with $a < c < b$. Indeed take a rational c with $a\sqrt{2} < c < b\sqrt{2}$, then $a < \frac{c}{\sqrt{2}} < b$.

3 Sequences

Definition. A *sequence* is an enumerated collection of objects in which repetitions are allowed and order matters. We write $a_1, a_2, a_3, \ldots$ or $(a_n)_{n=1}^{\infty}$.

What does it mean for a sequence $a_1, a_2, \ldots$ to tend to a limit ℓ? It is *not* enough that the terms a_n get closer to ℓ, for example, would not want $\frac{1}{2}$, $\frac{3}{4}$, $\frac{4}{5}$, $\ldots$to tend to 37. And it is *not* enough that the a_n get arbitrarily close to ℓ, $\forall \varepsilon > 0$, $\exists n \in \mathbb{N}$ such that $\ell - \varepsilon < a_n < \ell + \varepsilon$, for example would not want $\frac{1}{2}, 10, \frac{2}{3}, 10, \frac{3}{4}, 10, \ldots$ to tend to 1. We want the sequence to get *and stay* within ε of ℓ.

Definition (Limits)**.** We say that the sequence $a_1, a_2, a_3, \ldots$ tends to the limit $\ell \in \mathbb{R}$ as n tends to infinity if, $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, $\ell - \varepsilon < a_n < \ell + \varepsilon$.



More compactly: $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ such that $\forall n \geq N$,

$$|a_n - \ell| < \varepsilon.$$

Notation. The *absolute value* $|x|$ of $x \in \mathbb{R}$ is defined by

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

We think of $|a-b|$ as the "distance between a and b on the number line", for example $|2-9| = |9-2| = 7$. It is easy to check the triangle inequality

$$|a - b| \leq |a - c| + |c - b|.$$

When a_n tends to ℓ as n tends to infinity, we also write "$a_n \to \ell$ as $n \to \infty$" or "$\lim_{n\to\infty} a_n = \ell$" or "$(a_n)_{n=1}^{\infty}$ converges to ℓ". If there is a limit ℓ but it is not specified, we simply say "$(a_n)_{n=1}^{\infty}$ converges".

If $(a_n)_{n=1}^{\infty}$ does not converge , then we say it *diverges.*

Examples

(1) $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$, so $a_n = 1 - \frac{1}{n}$. Given $\varepsilon > 0$, choose $N > \frac{1}{\varepsilon}$ (by the Axiom of Archimedes). If $n \in \mathbb{N}$, then

$$|a_n - 1| = \left|1 - \frac{1}{n} - 1\right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon.$$

Hence $a_n \to 1$ as $n \to \infty$.

(2) $0, \frac{1}{2}, 0, \frac{1}{4}, \frac{1}{6}, \ldots$ defined by

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

Given $\varepsilon > 0$, pick $N > \frac{1}{\varepsilon}$. If $n \geq N$, then

$$|a_n - 0| \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon.$$

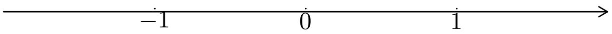
Hence $a_n \to 0$ as $n \to \infty$.

(3) $\frac{1}{2}, \frac{1}{2} + \frac{1}{4}, \frac{1}{2} + \frac{1}{4} + \frac{1}{8}, \ldots$, and we can verify by induction that $a_n = 1 - \frac{1}{2^n}$. Given $\varepsilon > 0$, choose $N > \frac{1}{\varepsilon}$. If $n \geq N$, then

$$|a_n - 1| = \frac{1}{2^n} \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon.$$

Hence $a_n \to 1$ as $n \to \infty$.

(4) $-1, 1, -1, 1, -1, 1, \ldots$ defined by $a_n = (-1)^n$



If a_n does not tend to ℓ, we write "$a_n \not\to \ell$". We say that it is divergent (note: it does not mean "goes off to infinity").

We implicitly assumed that if a limit exists, then it is unique. We'll prove this now. *Proof.* Suppose $a_n \to \ell$ and $a_n \to k$ as $n \to \infty$, with $l \neq k$. Choose $\varepsilon = \frac{1}{2}|\ell - k|$. Then $\exists N \in \mathbb{N}$ such that $|a_n - \ell| < \varepsilon \ \forall n \geq N$ and $\exists M \in \mathbb{N}$ such that $|a_n - k| < \varepsilon \ \forall n \geq M$. But then for any $n \geq \max\{N, M\}$,

$$2\varepsilon = |\ell - k| \leq |a_n - \ell| + |a_n - k| < 2\varepsilon \qquad \text{※}$$

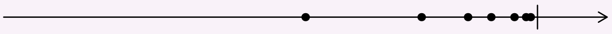
□

A sequence is *bounded* if there is a real number B such that $|a_n| \leq B$ for all $n \in \mathbb{N}$.

Notice that a convergent sequence is bounded; for if $a_n \to \ell$ as $n \to \infty$, then $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, $|a_n - \ell| < 1$. Hence $|a_n| \leq \max\{|a_1|, |a_2|, \ldots, |a_{N-1}|, |\ell| + 1\}$.

We say a sequence $(a_n)_{n=1}^{\infty}$ is *monotonic* if it is either increasing or decreasing. It is *increasing* if $a_{n+1} \geq a_n \ \forall n \in \mathbb{N}$.

Theorem (5). Every bounded monotonic sequence converges.



Proof. Suppose (a_n) is increasing. Then the set $\{a_n : n \geq 1\}$ is non-empty and is bounded above (because (a_n) is bounded), so it has a supremum ℓ, say. Given $\varepsilon > 0$, $\ell - \varepsilon$ is no an upper bound for $\{a_n : n \geq 1\}$, so there is some $N \in \mathbb{N}$ with $a_N > \ell - \varepsilon \ \forall n \geq \mathbb{N}$. Thus $\ell - \varepsilon < a_n < \ell \ \forall n \in \mathbb{N}$. Hence for all $n \geq N$, $|a_n - \ell| < \varepsilon$, so $a_n \to \ell$. Decreasing case is similar. □

Remarks

(1) Note that for an increasing sequence to converge, we only need to know that it is bounded above.

(2) The sequence (a_n) with $a_n = n$ is increasing but not bounded (and in fact, it diverges).

(3) Theorem 5 is in fact equivalent to the least Upper Bound Axiom.

(4) Can show that every sequence has a monotonic subsequence.

Proposition (6)**.** If $a_n \leq d \ \forall n$ and $a_n \to c$ as $n \to \infty$, then $c \leq d$.

Proof. Suppose $c > d$. Let $\varepsilon = |c - d|$. Then $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, $|a_n - c| < \varepsilon$. But $|a_n - c| < \varepsilon \implies a_n > d$. ※ □

Remark. If $a_n < d \ \forall n$ and $a_n \to c$ as $n \to \infty$, we need not have $c < d$. For example, $\frac{1}{2}, \frac{1}{2} + \frac{1}{4}, \frac{1}{2} + \frac{1}{4} + \frac{1}{8}, \ldots$ Each term is < 1, but $\lim_{n\to\infty} a_n = 1$.

Proposition (6)**.** If $a_n \to c$ as $n \to \infty$ and $b_n \to d$ as $n \to \infty$, then $a_n + b_n \to c + d$ as $n \to \infty$.

Proof. Given $\varepsilon > 0$ $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, $|a_n - c| < \frac{\varepsilon}{2}$ and $\exists M \in \mathbb{N}$ such that $\forall n \geq M$, $|b_n - d| < \frac{\varepsilon}{2}$. Choose $N^* = \max\{M, N\}$. Then $\forall n \geq N^*$,

$$\begin{aligned} |a_n + b_n - (c + d)| &\leq |a_n - c| + |b_n - d| \\ &\leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

□

3.1 Series

In the reals, the sum of two numbers is defined, so by induction, finite sums are defined. But infinite sums are not! Nevertheless, for example

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\cdots=\log 2.$$

Let (a_n) be a sequence. Then $s_k=\sum_{n=1}^{k}a_n$ is the k-th partial sum of the *series* whose n-th term is a_n. We write $\sum_{n=1}^{\infty}a_n=\lim_{k\to\infty}s_k$ if the limit exists.

Examples

(1) The series whose n-th term is $a_n=r^N$, for some $|r|<1$, is known as the *geometric series.*

$$\begin{aligned}s_k&=r+r^2+r^2+\cdots+r^k\\&=r\cdot\frac{1-r^k}{1-r}\\&\to\frac{r}{1-r}\end{aligned}$$

as $k\to\infty$ since $r^k\to 0$. Hence $\sum_{n=1}^{\infty}r^n=\frac{r}{1-r}$.

(2) The series whose n-th term is given by $a_n=\frac{1}{n}$ is known as the *harmonic series.*

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

In general,

$$\frac{1}{2^m+1}+\frac{1}{2^m+2}+\cdots+\frac{1}{2^{m+1}}\geq\frac{2^m}{2^{m+1}}=\frac{1}{2}.$$

Hence $S_{2^k}\geq 1+\frac{k}{2}$. So the partial sums are increasing and unbounded, so $\sum_{n=1}^{\infty}\frac{1}{n}$ diverges.

(3) $a_n=\frac{1}{n^2}$

$$S_{2^k-1}=1+\underbrace{\frac{1}{2^2}+\frac{1}{3^2}}_{\leq 2\cdot\frac{1}{2^2}}+\underbrace{\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\frac{1}{7^2}}_{\leq 4\cdot\frac{1}{4^2}}+\cdots+\frac{1}{(2^k-1)^2}$$

In general,

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

so

$$s_{2^k-1} \leq 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{k-1}} < 2$$

by example (1). By Theorem 5, $\sum_{n=1}^\infty \frac{1}{n^2}$ converges as partial sums increasing and bounded above. In fact $\sum_{n=1}^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$.

3.2 Decimal Expansions

Let (d_n) be a sequence with $d_n \in \{0, 1, 2, \ldots, 9\}$. Then $\sum_{n=1}^\infty \frac{d_n}{10^n}$ converges to some limit r, where $0 \leq r < 1$, because the partial sums $s_m = \sum_{n=1}^m \frac{d_n}{10^n}$ are increasing and bounded by

$$\sum_{n=1}^\infty \frac{9}{10^n} = \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} = 1.$$

We say that $0.d_1d_2d_3\ldots$ is the *decimal expansion* of r.

Does every x, $0 \leq x < 1$, have a decimal expansion?

Pick $d_1 \in \mathbb{Z}$ maximal such that $\frac{d_1}{10} \leq x < 1$. Then $d_1 \leq 9$ because $x < 1$ and $x - \frac{d_1}{10} < \frac{1}{10}$ because d_1 maximal. Now pick $d_2 \in \mathbb{Z}$ maximal such that

$$\frac{d_2}{100} \leq x - \frac{d_1}{10}.$$

Then $d_2 \leq 9$ because $x - \frac{d_1}{10} < \frac{1}{10}$ and

$$x - \frac{d_2}{10} - \frac{d_2}{100} < \frac{1}{100}$$

because d_2 maximal. Inductively, pick $d_n \in \mathbb{Z}$ maximal with

$$\frac{d_n}{10^n} \leq x - \sum_{j=1}^{n-1} \frac{d_j}{10^j}$$

so $0 \leq x - \sum_{j=1}^n \frac{d_j}{10^j} < \frac{1}{10^n}$. Since $\frac{1}{10^n} \to 0$ as $n \to \infty$, $x - \sum_{j=1}^n \frac{d_j}{10^j} \to 0$, i.e.

$$x = \sum_{j=1}^\infty \frac{d_j}{10^j} = 0.d_1d_2d_3\ldots$$

Remarks

(1) Decimal expansions need not be unique, e.g. $0.47999\cdots = 0.48000\ldots$
Suppose $0.a_1a_2a_3\cdots = 0.b_1b_2b_3\ldots$. We may suppose $a_j = b_j$ for $j < K$ for some K and $a_K < b_K$. Then

$$\sum_{j=k+1}^\infty \frac{a_j}{10^j} \leq \sum_{j=k+1}^\infty \frac{9}{10^j} = \frac{9}{10^{k+1}} \cdot \frac{1}{1 - \frac{1}{10}} = \frac{1}{10^k}.$$

Hence we must have $b_k = a_k + 1$ and $a_j = 0$, $b_j = 0$ $\forall j > K$.

(2) A decimal expansion is *periodic* if, after a finite number of terms, say l digits, it repeats in blocks, of length k say, i.e. $\exists l, k$ such that $d_{n+k} = d_n$ $\forall n > l$.

A periodic decimal is rational, for example

$$\begin{aligned} x &= 0.7832147147147147\ldots \\ 10^4 x - 7832 &= 0.147147147147\ldots \\ &= 147 \sum_{j=1}^{\infty} \frac{1}{10^{3j}} \\ &= 147 \cdot \frac{1}{10^3} \cdot \frac{1}{1 - \frac{1}{10^3}} \end{aligned}$$

so $x \in \mathbb{Q}$.

Conversely, if $x \in \mathbb{Q}$, then x has a periodic decimal expansion. To see this, we write $x = \frac{p}{2^a 5^b q}$ where $a, b, p, q \in \mathbb{Z}$, $a, b, q \geq 0$, $(q, 10) = 1$. Then $10^{\max(a,b)} x = \frac{t}{q} = n = \frac{c}{q}$, where $n \in \mathbb{Z}$, $c \in \mathbb{Z}$ and $0 \leq c < q$. By Fermat-Euler, $10^{\phi(q)} \equiv 1 \pmod{q}$ or $10^{\phi(q)} - 1 = kq$ for some $k \in \mathbb{N}$. Hence

$$\frac{c}{q} = \frac{kc}{kq} = \frac{kc}{10^{\phi(q)} - 1} = kc \sum_{j=1}^{\infty} \frac{1}{(10^{\phi(q)})^j}$$

Since $0 \leq kc < kq$, we can write kc as a $\phi(q)$-digit number $d_1 d_2 \ldots d_{\phi(q)}$. Then

$$\frac{c}{q} = 0.d_1 d_2 \ldots d_{\phi(q)} d_1 d_2 \ldots d_{\phi(q)} d_1 \ldots$$

and so x is periodic.

3.3 Euler's number e

Define

$$e = 1 + \frac{1}{1!} + \underbrace{\frac{1}{2!}}_{=\frac{1}{2}} + \underbrace{\frac{1}{3!}}_{\leq\frac{1}{4}} + \underbrace{\frac{1}{4!}}_{\leq\frac{1}{8}} + \cdots$$

Note that by Theorem 5 this series converges, because the partial sums are increasing and bounded by

$$1 + 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 3$$

If we define $0! = 1$, then

$$e = \sum_{j=0}^{\infty} \frac{1}{j!}.$$

Proposition (7)**.** e is irrational.

Proof. Suppose e were rational, i.e. $e = \frac{p}{q}$ where $p, q \in \mathbb{N}$ and $q > 1$ since $2 < e < 3$. Then $q!e \in \mathbb{N}$. But

$$\begin{aligned} q!e &= \underbrace{q! + \frac{q!}{1!} + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{q!}}_{\in \mathbb{N}} + \underbrace{\frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \cdots}_{\text{show: } < 1} \\ &= N + x \end{aligned}$$

where

$$\begin{aligned} x &= \sum_{j=q+1}^{\infty} \frac{q!}{j!} \\ &= \sum_{j=1}^{\infty} \frac{q!}{(q+j)!} \\ &= \frac{1}{q+1} + \underbrace{\frac{1}{(q+1)(q+2)}}_{\leq \frac{1}{(q+1)^2}} + \underbrace{\frac{1}{(q+1)(q+2)(q+3)}}_{\leq \frac{1}{(q+1)^3}} + \cdots \end{aligned}$$

an in general $\frac{q!}{(q+j)!} \leq \frac{1}{(q+1)^j}$, so

$$x \leq \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+)^3} + \cdots = \frac{1}{q} < 1$$

as $q \geq 2$. Hence $0 < x < 1$, contradicting that $q!e \in \mathbb{N}$, so e is irrational. □

We say a real number x is *algebraic* if it is a root of a (non-zero) polynomial with integer coefficients (or rational coefficients - same thing!).

Examples

(1) Every rational number is algebraic:

$$x = \frac{p}{q} \implies qx - p = 0$$

(2) $\sqrt{2}$ is algebraic: it satisfies $x^2 - 2 = 0$.

A real number is *transcendental* if it is not algebraic.

Theorem ((9) Liouville 1851)**.** The number $L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

We will need two facts about polynomials.

Lemma (Fact A)**.** For any polynomial p, $\exists$ constant K such that

$$|p(x) - p(q)| \leq K|x - y| \qquad \forall 0 \leq x, y \leq 1.$$

Proof. Suppose

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0.$$

Then

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

so

$$|p(x) - p(y)| \leq |x - y|[(|a_d| + |a_{d-1}| + \cdots + |a_1|) \cdot d].$$

□

Lemma (Fact B)**.** A non-zero polynomial of degree d has at most d roots.

Proof. Given a polynomial p of degree d, we may assume that the fact holds for all polynomials of degree $< d$ and that p has a root a, say (otherwise we're done). By long division, we may write

$$p(x) = (x - a)q(x)$$

for some polynomial q of degree $d - 1$. So each root of p is either a or a root of q. But by the induction hypothesis, q has at most $d - 1$ roots. □

Proof of Theorem 9. Write

$$L_n = \sum_{k=0}^{n} \frac{1}{10^{k!}}$$

so $L_n \to L$. Suppose there is a polynomial p of which L is a root. Then by Fact A, there exists K such that $|p(x) - p(y)| \leq K|x - y|$ $\forall 0 \leq x, y \leq 1$. Note

$$|L - L_n| = \sum_{k=n}^{\infty} \frac{1}{10^{k!}} \leq \frac{2}{10^{(n+1)!}}.$$

Suppose p has degree d, i.e. $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$, $a_d \neq 0$. Notice that

$$L_n = \frac{s}{10^{n!}}$$

for some $s \in \mathbb{N}$, so $p(L_n) = \frac{t}{10^{dn!}}$ for some $t \in \mathbb{N}$. By Fact B, for sufficiently large n, L_n is not a root of p. Hence

$$|p(L_n)| \geq \frac{1}{10^{dn!}}$$

i.e. $|p(L_n) - p(L)| \geq \frac{1}{10^{dn!}}$. Therefore

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

a contradiction for sufficiently large n. □

Remarks

(1) The same proof shows that any real number x such that $\forall n \in \mathbb{N}$, $\exists$ rational $\frac{p}{q}$ with

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$$

is transcendental.
"x has a very god rational approximation $\implies$ transcendental"

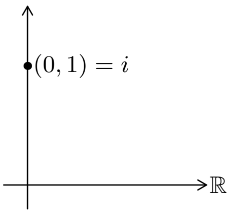
(2) Such x are known as *Liouville numbers.*

(3) This proof does not show that e is transcendental, but in fact it is.

(4) We will give another proof of the existence of transcendental numbers in Chapter IV.

3.4 Complex Numbers

Since polynomials have no real roots, e.g. $x^2 + 1$. We will try to define x with $x^2 = -1$ "into existence".



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

$$(a, b) + (c, d) = (a + c, b + d)$$

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

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

$$(a, 0) + (b, 0) = (a + b, 0)$$

$$(a, 0) \cdot (b, 0) = (ab, 0)$$

Now let $i = (0, 1)$. Then

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0).$$

Note that every $z \in \mathbb{Z}$ is of the form $a = bi$ with $a, b \in \mathbb{R}$. Indeed,

$$(a, b) = a(1, 0) + b(0, 1) = a + bi.$$

Remarks

(1) $\mathbb{C}$ obeys all the usual rules of arithmetic. In particular, it obeys (1)-(3) as set out for $\mathbb{R}$, including that $\forall z \neq 0$, $\exists w$ such that $zw = 1$. Indeed, given $z = a + bi$, note that

$$(a + bi)(a - bi) = a^2 + b^2 \implies (a + bi)\frac{a - bi}{a^2 + b^2} = 1.$$

A structure obeying rules (1)-(3) is called a *field*, e.g. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$ with p a prime, but *not* $\mathbb{Z}$!

(2) Every non-zero polynomial (even allowing complex coefficients) has a root in $\mathbb{C}$. This is known as the Fundamental Theorem of Algebra.

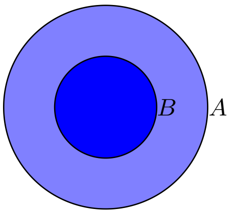
CHAPTER III: Sets, Functions and Relations

4 Sets, Functions and Relations

A *set* is a collection of mathematical objects. For example $\mathbb{R}$, $\mathbb{N}$, $\{1, 5, 9\}$, $[-2, 3]$. The order of elements in the set is immaterial, and elements are only counted once. For example

$$\{1, 3, 7\} = \{1, 7, 3\} \qquad \text{and} \qquad \{3, 4, 48\} = \{3, 4, 8\}.$$

We write $x \in A$ if x is an element of the set A, and $x \notin A$ if not. Two sets are equal if they have the same elements. That is, if $\forall x,\ x \in A \iff x \in B$, then $A = B$. In particular, there is only one empty set $\emptyset$. A set B is a *subset* of A, written "$B \subseteq A$" or "$B \subset A$", if every element of B is an element of A.

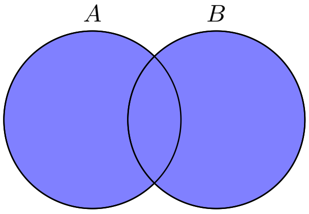


B is said to be a *proper* subset of A if $B \subseteq A$ and $B \neq A$ (also write $B \subsetneq A$).

Note that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. If A is a set and P is a property of (some) elements of A, we can write $\{x \in A : P(x)\}$ for the subset of A comprising those elements for which $P(x)$ holds. For example $\{n \in \mathbb{N} : n \text{ is prime}\} = \{2, 3, 5, 7, 11, \dots\} \subseteq \mathbb{N}$.

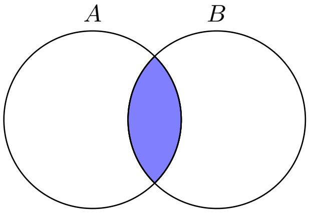
If A and B are sets, then their *union* $A \cup B$ is

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$



Their *intersection* $A \cap B$ is defined to be

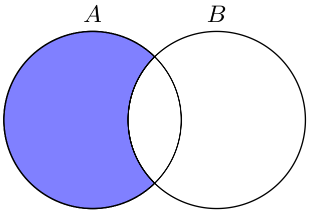
$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$



We say A and B are *disjoint* if $A \cap B = \emptyset$. Note that we can view intersection as a special case of subset selection:

$$A \cap B = \{x \in A : x \in B\}.$$

Similarly, have the *set difference* $A \setminus B = \{x \in A : x \notin B\}$. "$A$ but not B" or "A minus B".



Note that $\cup$ and $\cap$ are commutative and associative. Also, $\cup$ is distributive over $\cap$, i.e.

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

and $\cap$ is distributive over $\cup$, i.e.

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

To prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, show that $LHS \subseteq RHS$ and $RHS \subseteq LHS$, so $LHS = RHS$.
If $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$, so $x \in A$ and ($x \in B$ or $x \in C$). If $x \in B$, then $x \in A \cap B$, and if $x \in C$, then $x \in A \cap C$. Hence, in any case, $x \in (A \cap B) \cup (A \cap C)$. Conversely, if $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap B$ or $x \in A \cap C$. If $x \in A \cap B$, then $x \in A$ and $x \in B \cup C$. If $x \in A \cap C$, then $x \in A$ and $x \in B \cup C$, so in any case $x \in A \cap (B \cup C)$. □

If $A_1, A_2, A_3, \ldots$ are sets, then

$$\begin{aligned}\bigcap_{n=1}^{\infty} A_n &= A_1 \cap A_2 \cap A_3 \cap \cdots \\ &= \{x : x \in A_n \text{ for all } n \in \mathbb{N}\}\end{aligned}$$

Similarly,

$$\begin{aligned}\cup_{n=1}^{\infty} A_n &= A_1 \cup A_2 \cup A_3 \cup \cdots \\ &= \{x : x \in A_n \text{ for some } n \in \mathbb{N}\}\end{aligned}$$

Remark. $\cup_{n=1}^{\infty} A_n$ is *not* the "limit" of anything!

More generally, given an index set I and a collection of sets A_i indexed by I, we write

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

and

$$\cup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\}.$$

Given sets A and B, we can form their *Cartesian product*

$$A \times B = \{(a, b) : a \in A, b \in B\},$$

which is the set of *ordered pairs* (a, b) with $a \in A$, $b \in B$. Here $(a, b) = (a', b') \iff a = a' \wedge b = b'$. [Note we can define $(a, b) = \{a, \{a, b\}\}$]. We can extend to ordered triples and so on, for example

$$\begin{aligned} \mathbb{R}^3 &= \mathbb{R} \times \mathbb{R} \times \mathbb{R} \\ &= \{(x, y, z) : x \in \mathbb{R}, y \in \mathbb{R}, z \in \mathbb{R}\} \end{aligned}$$

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

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

For example, if $X = \{1, 2\}$, then $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Remark. Given a set A, we can form $\{x \in A : P(c)\}$ for any property P. But we *cannot* form $\{x : P(X)\}$. Indeed suppose

$$X = \{x : x \text{ is a set and } x \notin x\}$$

were a set. Then $X \in X$ implies that $X \notin X$ ⨳, but $X \notin X$ implies that $X \in X$ ⨳. This is known as *Russell's Paradox*. Similarly, there is not 'universal' set Y, meaning that $\forall x, x \in Y$. Otherwise we 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 from known sets (e.g. $\mathbb{N}$, $\mathbb{R}$) in one of the ways described above.

4.1 Finite Sets

Write

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$$

Given $n \in \mathbb{N}_0$, we say a set A has *size* n if we can write $A = \{a_1, a_2, \dots, a_n\}$ with the elements a_i distinct. For example, $\{1, 3, 7\}$ has size 3, $\emptyset$ has size 0.

We say A is *finite* if $\exists n \in \mathbb{N}_0$ such that A has size n, and A is *infinite* otherwise.

Proposition 1. A set of size n has exactly 2^n subsets.

Proof 1. May assume that our set is $\{1, 2, \ldots, n\}$. To specify a subset S of $\{1, 2, \ldots, n\}$ we must say if $1 \in S$ or $1 \notin S$, then if $2 \in S$ or $2 \notin S$, and so on. Hence the number of choices for S is

$$\underbrace{2}_{1\in S?} \cdot \underbrace{2}_{2\in S?} \cdot \underbrace{2}_{3\in S?} \cdots \underbrace{2}_{n\in S?} = 2^n.$$

□

Proof 2. By induction on n. Clearly true for $n = 0$. Given $n > 0$, and $T \subseteq \{1, 2, \ldots, n-1\}$, how many $S \subseteq \{1, 2, \ldots, n\}$ are there such that $S \cap \{1, \ldots, n-1\} = T$? There are exactly 2, namely T and $T \cup \{n\}$. Hence the number of subsets of $\{1, 2, \ldots, n\}$ is

$$2 \times \text{number of subsets of } \{1, 2, \ldots, n-1\} = 2 \cdot 2^{n-1} = 2^n$$

□

If A has size n we write "$|A| = n$" or "$\#A = n$".
So Proposition 1 says that $|A| = n \implies |\mathcal{P}(A)| = 2^n$.

Given $n \in \mathbb{N}_0$ and $0 \leq k \leq n$, we write $\binom{n}{k}$ "n choose k" for the number of subsets of an n-element set that are of size k. In other words,

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

$\binom{n}{k}$ is called a *binomial coefficient*. For example, the subsets of size 2 of $\{1, 2, 3, 4\}$ are precisely

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

so $\binom{4}{2} = 6$. Note that by definition $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, $\binom{n}{1} = n$ $(n > 0)$ and also

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Also, we have $\binom{n}{k} = \binom{n}{n-k}$ $\forall n \in \mathbb{N}_0, 0 \leq k \leq n$. For example $\binom{8}{3} = \binom{8}{5}$. Indeed, specifying which k elements to pick is the same as specifying which $n - k$ elements *not* to pick. Moreover,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \forall n \in NN, 1 \leq k \leq n-1.$$

For example, $\binom{8}{3} = \binom{7}{2} + \binom{7}{3}$. Indeed, the number of subsets of $\{1, 2, \ldots, n\}$ of size k that do not include n is $\binom{n-1}{k}$, while the number of subsets of $\{1, 2, \ldots, n\}$ of size k that

do include n is $\binom{n-1}{k-1}$.
We obtain Pascal's Triangle:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \cdots & & & & &
\end{array}$$

The n-th row contains the numbers $\binom{n}{k}$. Each row starts and ends with a 1, and the remaining entries are the sum of the two terms immediately above.

Proposition 2.

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

Proof. Given a set of size n, there are $n(n-1)(n-2)\cdots(n-k+1)$ ways to pick k elements, one by one, in order. But each subset of size k is picked in $k(k-1)(k-2)\cdots 2\cdot 1$ ways by this method. Hence the number of subsets of size k in $\{1,2,\ldots,n\}$ is

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots 2\cdot 1}.$$

□

Note that the formula tells us, for example, that

$$\binom{n}{2} = \frac{n(n-1)}{2} \sim \frac{n^2}{2}$$

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6} \sim \frac{n^3}{6}$$

for large n.

Theorem 2 (Binomial Theorem)**.** For all $a, b \in \mathbb{R}$, $n \in \mathbb{N}$

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

Proof. When we expand

$$(a+b)^n = (a+b)(a+b)\cdots(a+b)$$

we obtain terms of the form $a^{n-k}b^k$ $(0 \leq k \leq n)$ and the number of terms of the form $a^{n-k}b^k$ is $\binom{n}{k}$ as we must specify k brackets from which to pick b. Hence

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

□

Example.

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

so for small x, a good approximation to $(1+x)^n$ is $1+nx$, for example $(1.00001)^8 \approx 1.00008$. A better approximation is $1 + nx + \frac{n(n-1)}{2}x^2$, for example $(1.00001)^8 \approx 1.00008 + 28(0.00001)^2$.

What can we say about the relationship between sizes of unions and intersections of finite sets?
For example

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

Also,

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

Theorem (Inclusion-Exclusion Principle)**.** Let $S_1, S_2, \ldots, S_n$ be finite sets. Then

$$|S_1 \cup S_2 \cup \cdots \cup S_n| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \cdots + (-1)^{n+1} \sum_{|A|=n} |S_A|,$$

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. Equivalently,

$$|\cup_{i=1}^{n} S_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{A \subseteq \{1,2,\ldots,n\} \\ |A|=k}} \left| \bigcap_{i \in A} S_i \right|.$$

Proof. Let $x \in S_1 \cup S_2 \cup \cdots \cup S_n$, say $x \in S_i$ for k of the S_i. We want x to be counted exactly once in the RHS. Indeed,

$$\#\{A : |A| = 1 \text{ with } x \in S_A\} = k,$$

and

$$\#\{A : |A| = 2 \text{ with } x \in S_A\} = \binom{k}{2}$$

and in general,

$$\#\{A : |A| = r \text{ with } x \in S_A\} = \binom{k}{r}$$

for $r \leq k$, and $= 0$ for $r > k$. Thus the number of times x is counted on the RHS is

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

for $k \geq 1$ (and $k = 0$ doesn't happen since x is in the union). □

4.2 Functions

Given sets A and B, a function f from A to B is a "rule" that assigns to every $x \in A$ a unique element $f(x) \in B$.

More formally, a *function* from A to B is a subset $f \subseteq A \times B$ such that for all $x \in A$, there is a unique $y \in B$ such that $(x, y) \in f$.
If f is a function from A to B, we write $f : A \to B$. If $(x, y) \in f$, we can write $f(x) = y$ or $x \mapsto y$.

Examples

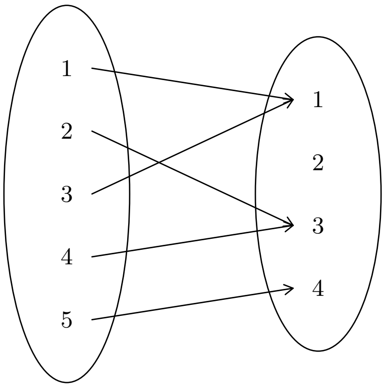
(1) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is a function.

(2) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{1}{x}$ is *not* a function ($f(0) = ?$)

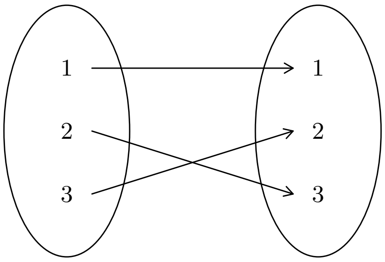
(3) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \pm\sqrt{|x|}$ is *not* a function.

(4) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \begin{cases} 1 & \text{if } x \text{ is rational} \\ 0 & \text{otherwise} \end{cases}$ is a function.

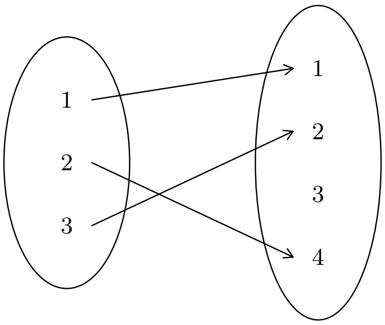
(5) $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4\}$ given by



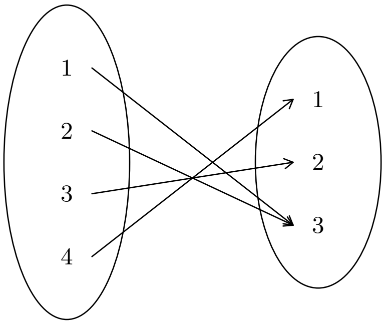
(6) $f : \{1, 2, 3\} \to \{1, 2, 3\}$



(7) $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$



(8) $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$



We say $f : A \to B$ is *injective* if $\forall a, a' \in A$, $a \neq a' \implies f(a) \neq f(a')$. Equivalently, f is injective if $f(a) = f(a') \implies a = a'$. Examples (5) and (8) are not injective, but (6) and (7) are.

We say $f : A \to B$ is *surjective* if $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$. Examples (5) and (7) are not surjective, but (6) and (8) are.

We say $f : A \to B$ is *bijective* if it is both injective and surjective. Example (6) is the only bijection. If $f : A \to B$ is a bijection, then everything in B is "hit" exactly once (that is, f pairs the elements of A and B). A *permutation* of A is a bijection $A \to A$.

Given $f : A \to B$, we say A is the *domain* of f and B is its *range*. The *image* of f is the set $f(A) = \{f(a) : a \in A\} = \{b \in B : f(a) = b \text{ for some } a \in A\}$. The image of f is also sometimes denoted $\mathrm{Im}(f)$. For example, if $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, then $\mathrm{Im}(f) = \{y \in \mathbb{R} : y \geq 0\}$.

When specifying a function we must specify its domain and range. For example "Is the function $f(x) = x^2$ injective?" is meaningless, as $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$ is injective, but $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$ is *not*.

Observations

(1) f is surjective if and only if $f(A) = B$. In particular, if $|B| > |A|$ then there can be not surjection from A to B.

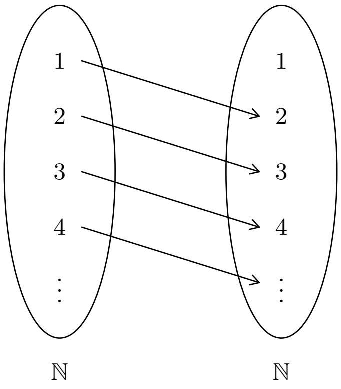
(2) There can be no injection from A to B is $|A| > |B|$.

(3) If $f : A \to A$, then f is injective if and only if f is surjective.

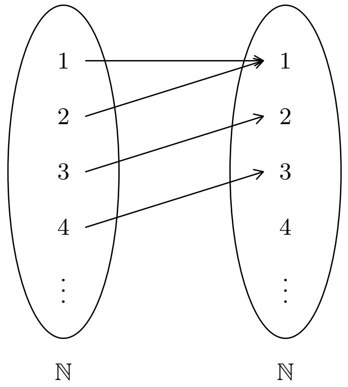
(4) There is no bijection from A to any proper subset of A.

Note that (3) and (4) do *not* hold for infinite sets:

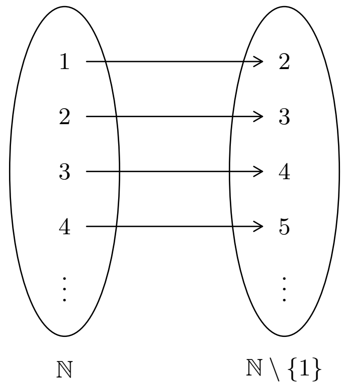
(a) $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ is injective but not surjective.



(b) $g : \mathbb{N} \to \mathbb{N}$, $x \mapsto \begin{cases} x - 1 & \text{if } x \neq 1 \\ 1 & \text{if } x = 1 \end{cases}$ is surjective but not injective.



(c) $h : \mathbb{N} \to \mathbb{N} \setminus \{1\}$, $x \mapsto x + 1$ is a bijection from $\mathbb{N}$ to a proper subset.



Further Examples

(i) For any set X, we have the *identity function* $\mathrm{id}_X : X \to X$, $x \mapsto x$.

(ii) Given a set X and $A \subseteq X$, we have the *indicator function* (or *characteristic function*) of A, $1_A : X \to \{0, 1\}$, $x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$

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

(iv) The operation $+$ on $\mathbb{N}$ is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto a + b$.

(v) A set X has size n if and only if there is a bijection $\{1, 2, \ldots, n\} \to X = \{a_1, \ldots, a_n\}$, $i \mapsto a_i$.

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

Notation. The notation "$g \circ f$" can be read as "g composed with f", or "g circle f" or "g after f".

For example if $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x$ and $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$ then $g \circ f(x) = g(f(x) = g(2x) = 2x + 1$ and $f \circ g(x) = f(g(x)) = f(x + 1) = 2(x + 1)$. So in general, $\circ$ is *not* commutative. In the example above, $f \circ g \neq g \circ f$ since $f \circ g(1) = 4 \neq 3 = g \circ f(1)$.

However, $\circ$ is associative, i.e. 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 every $x \in A$,

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

and

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

We may therefore drop the brackets and write $h \circ g \circ f$ without ambiguity.

We say $f : A \to B$ is *invertible* if $\exists g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Example. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x + 1$ and $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{x-1}{2}$. Indeed, $\forall x \in \mathbb{R}$,

$$(g \circ f)(X) = g(2x + 1) = \frac{2x + 1 - 1}{2} = x$$

so $g \circ f = \mathrm{id}_{\mathbb{R}}$. Also, $\forall x \in \mathbb{R}$,

$$(f \circ g)(x) = f\left(\frac{x-1}{2}\right) = 2\left(\frac{x-1}{2}\right) + 1 = x,$$

so $f \circ g = \mathrm{id}_{\mathbb{R}}$. Hence f is invertible with inverse g.

Note. For $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ and $g : \mathbb{N} \to \mathbb{N}$, $x \mapsto \begin{cases} x - 1 & \text{if } x \neq 1 \\ 1 & \text{if } x = 1 \end{cases}$. We have $g \circ f = \mathrm{id}_{\mathbb{N}}$ but $f \circ g \neq \mathrm{id}_{\mathbb{N}}$ because $f \circ g(1) \neq 1$.

We had said $f : A \to B$ is invertible if $\exists g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Given $f : A \to B$, when is there a map $g : B \to A$ such that $g \circ f = \mathrm{id}_A$? If such a g exists, and $a, a' \in A$ are such that $f(a) = f(a')$, then $gf(a) = gf(a')$, so $a = a'$. Thus f must be injective. Conversely, if f is injective, we can find g such that $g \circ f = \mathrm{id}_A$: $b \in f(A)$, let $g(b) = a$, where a is the unique element of A with $f(a) = b$; if $b \notin f(A)$, let $g(b)$ be anything you like.

Given $f : A \to B$, when is there a map $g : B \to A$ such that $f \circ g = \mathrm{id}_B$? We need $f(g(B))$, so f must be surjective. Conversely, if f is surjective, we can find $f : B \to A$ with $f \circ g = \mathrm{id}_B$: for each $b \in B$, pick some $a \in A$ with $f(a) = b$ and put $g(b) = a$.

It follows that $f : A \to B$ is invertible if and only if f is bijective. We write $f^{-1} : B \to A$ for the inverse of f when it exists.

Note. Given $f : A \to B$ and $U \subseteq B$, we sometimes write

$$f^{-1}(U) = \{a \in A : f(a) \in U\}$$

for the *preimage* of U. This does *not* mean that f has an inverse!

4.3 Relations

A relation on a set X is a subset $R \subseteq X \times X$. We usually write aRb for $(a, b) \in R$. (This is read as "a is related to b".)

Examples

of relations on $\mathbb{N}$.

(i) aRb if a, b have the same final digit;

(ii) aRb if $a \mid b$;

(iii) aRb if $a \neq b$;

(iv) aRb if $a = b = 1$;

(v) aRb if $|a - b| \leq 3$;

(vi) aRb if either $a, b \leq 4$ or $a, b \geq 5$.

There are three properties that a relation might have that are of special interest:

- R is *reflexive* if $\forall x \in X$, xRx.
- R is *symmetric* if $x, y \in X$, $xRy \implies yRx$.
- R is *transitive* if $\forall x, y, z \in X$, xRy and $yRz \implies xRz$.

Example	1	2	3	4	5	6
reflexive	✓	✓	✗	✗	✓	✓
symmtric	✓	✗	✓	✓	✓	✓
transitive	✓	✓	✗	✓	✗	✓

A relation R is an *equivalence relation* if it is reflexive, symmetric and transitive. We often write $a \sim b$ for aRb. So (1) and (6) are equivalence relations. We have already seen another one:

(7) $X = \mathbb{Z}$ with $a \sim b$ if $a \equiv b \pmod 5$.

This equivalence relation partitions $\mathbb{Z}$ into "pieces" consisting of related elements, namely

$$\{x \in \mathbb{Z} : x \equiv 0 \pmod 5\}, \{x \in \mathbb{Z} : x \equiv 1 \pmod 5\}, \ldots, \{x \in \mathbb{Z} : x \equiv 4 \pmod 5\}.$$

Given a set X a *partition* of X is a collection of pairwise disjoint subsets (called "parts") whose union is X.

If $\sim$ is an equivalence relation on X, then the *equivalence class* of $x \in X$ is

$$[x] = \{y \in Y : y \sim x\}.$$

For example in (1), $[376] = \{$all natural numbers ending in 6$\}$. In (7), $[12] = \{y : y \equiv 2 \pmod 5\}$.

Observation. Given a partition of X, there is an equivalence relation R whose equivalence classes are precisely the parts of the partition: just define $a \sim b$ if a and b lie in the same part.

Theorem 5. Let $\sim$ be any equivalence relation on X. Then the equivalence classes form a partition of X.

Proof. Since $\sim$ is reflexive, we have $x \in [x]\ \forall\ x \in X$. Thus

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

It remains to show that $\forall x, y \in X$, either $[x] \cap [y] = \emptyset$ or $[x] = [y]$. Suppose $[x] \cap [y] \neq \emptyset$, and let $z \in [x] \cap [y]$. Then $z \sim x$, so by symmetry $x \sim z$, and $z \sim y$. Thus by transitivity, $x \sim y$. Let now $w \in [y]$, so $y \sim w$. Since $x \sim y$ and $y \sim w$, by transitivity, $x \sim w$. Thus $w \in [x]$. Hence if $[x] \cap [y] \neq \emptyset$, then $[y] \subseteq [x]$. □

This is a useful viewpoint: it is now easy to see that there is an equivalence relation on $\mathbb{N}$ with 3 equivalence classes, of which 2 are infinite and 1 is finite - simply take a partition of $\mathbb{N}$ with this property.

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

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

For example in (7), X/R has size (5), in (1), X/R has size 10. In fact, this explains why we sometimes write $\mathbb{Z}/5\mathbb{Z}$ instead of $\mathbb{Z}_5$. The map $q : X \to X/R$, $x \mapsto [x]$ is the *quotient map* (or *projection map*).

Another example on $\mathbb{Z} \times \mathbb{N}$, define $(a, b)R(c, d)$ if $ad = bc$. It is easy to see that is an equivalence relation. For example

$$[(1, 2)] = \{(1, 2), (2, 4), (3, 6), \ldots\}$$

so we could regard $\mathbb{Z} \times \mathbb{N}/R$ as a copy of $\mathbb{Q}$, by identifying $[(a, b)]$ with $\frac{a}{b} \in \mathbb{Q}$. The quotient map $q : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{N}/R$, $(a, b) \mapsto \frac{a}{b}$.

5 Countability

We would like to talk about sizes of infinite sets, for example $\mathbb{N}$ "looks smaller than" $\mathbb{Z}$, and a lot smaller than $\mathbb{Q}$, which in turn looks smaller than $\mathbb{R}$.

We say a set X is *countable* if X is finite or there is a bijection $X \to \mathbb{N}$. That is, X is countable if and only if we can list the elements of X as $x_1, x_2, x_3, \dots$ (might terminate).

Examples

(1) Any finite set is countable.

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

(3) $\mathbb{Z}$ is countable, as we may list $\mathbb{Z}$ as

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

i.e.

$$x_n = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Lemma 1. Any subset of $\mathbb{N}$ is countable

Proof. If $S \subseteq \mathbb{N}$ is non-empty, by Well Ordering Principle there is a least element $s_1 \in S$. If $S \setminus \{s_1\} \neq \emptyset$, by Well Ordering Principle there is a least element $s_2 \in S \setminus \{s_1\}$. If $S \setminus \{s_1, s_2\} \neq \emptyset$, ...
If at some point this process stops, then $S = \{s_1, s_2, \dots, s_m\}$ is finite. If it goes on forever, the map $g : \mathbb{N} \to S$ given by $g(n) = s_n$ is well-defined (for every n, there is a unique s_n) and is injective. It is also surjective because if $k \in S$, then $k \in \mathbb{N}$, and there are $< k$ elements of S less than k, so $k = s_n$ for some $n \leq k$. □

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

$$S = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots \right\} \cup \{1\},$$

then S is countable as we can list it as

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

but if we had tried to list the elements in increasing order (as in the proof of Lemma 1) then I would not list all the list.

Theorem 2. The following statements are equivalent:

(i) X is countable;

(ii) there is an injection $X \to \mathbb{N}$;

(iii) $X = \emptyset$ or there is a surjection $\mathbb{N} \to X$.

Proof. Plainly (i) $\implies$ (ii) for if X is finite, it obviously injects into $\mathbb{N}$, and if X bijects with $\mathbb{N}$, then it certainly injects into $\mathbb{N}$.
Conversely, if there is an injection $f : X \to \mathbb{N}$, then f is a bijection between X and $S = f(X)$. If S is finite, then so is X. If S is infinite, then by Lemma 1, there is a bijection $g : S \to \mathbb{N}$, and thus $X \to^f S = f(X) \to^g \mathbb{N}$ is a bijection. So (ii) $\implies$ (iii).
Plainly (iii) $\implies$ (i), if $X \neq \emptyset$ and there is a surjection $f : \mathbb{N} \to X$, define $g : X \to \mathbb{N}$ by $g(a) = \min f^{-1}(\{a\})$, which exists by the Well Ordering Principle. Since g is injective, so by (ii) $\implies$ (i), X is countable, i.e. (iii) $\implies$ (i). □

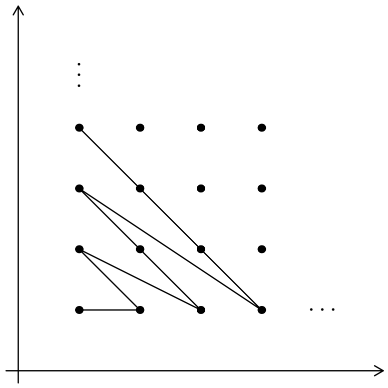
Corollary 3. Any subset of a countable set is countable.

Proof. If $Y \subseteq X$ and X is countable, then take the injection $X \to \mathbb{N}$ restricted to Y. □

Theorem 4. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof 1. Define $a_1 = (1, 1)$ and a_n inductively by writing

$$a_{n-1} = (p, q), \qquad a_n = \begin{cases} (p-1, q+1) & p \neq 1 \\ (1, p+q) & \text{otherwise} \end{cases}$$



This list includes every point $(x, y) \in \mathbb{N} \times \mathbb{N}$ by induction on $x + y$. □

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

Corollary 5. $\mathbb{Z} \times \mathbb{Z}$ is countable.

Proof. Since $\mathbb{Z}$ is countable, there is an injection $\mathbb{Z} \to \mathbb{N}$, so because $\mathbb{N} \times \mathbb{N}$ is countable, we have an injection

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}.$$

□

By induction, $\mathbb{Z}^k$ is countable for any $k \in \mathbb{N}$.

Theorem 6. A countable union of countable sets is countable.

Proof 1. May assume that our countable sets are indexed by $\mathbb{N}$, so given countable sets $A_1, A_2, A_3, \ldots$, we wish to show $\bigcup_{n \in \mathbb{N}} A_n$ is countable.
For each $i \in \mathbb{N}$, since A_i is countable, may list its elements as

$$a_1^{(i)}, a_2^{(i)}, a_3^{(i)}, \ldots$$

(might terminate). Define

$$f : \bigcup_{n \in \mathbb{N}} A_n \to \mathbb{N}, \qquad x \mapsto 2^i 3^j.$$

where $x = a_j^{(i)}$ for the least i satisfying $x \in A_i$ (as x could be in more than one of the A_i). This is an injection. □
Proof 2. Let I be a countable index set, and for each $i \in I$, A_i is a countable set. Since I is countable, there is an injection $f : I \to \mathbb{N}$, and for each $i \in I$, since A_i is countable, there is an injection $g_i : A_i \to \mathbb{N}$. We construct an injection $h : A = \bigcup_{i \in I} A_i \to \mathbb{N} \times \mathbb{N}$ as follows: for each $x \in A$, pick $m_x = \min\{j \in \mathbb{N} : x \in A_i, f(i) = j\}$, which exists by Well Ordering Principle. Let i_x be such that $f(i_x) = m_x$ (i_x is unique because f is injective). Set $h(x) = (m_x, g_{i_x}(x))$. This h is an injection. □

Example.

$$\mathbb{Q} = \bigcup_{n \in \mathbb{N}} \frac{1}{n}\mathbb{Z} = \bigcup_{n \in \mathbb{N}} \left\{\frac{m}{n} : m \in \mathbb{Z}\right\},$$

so $\mathbb{Q}$ is a countable union of countable sets, hence countable.

Theorem 7. The set $\mathbb{A}$ of algebraic numbers is countable.

Proof. It suffices to show that the set of all polynomials with integer coefficients is countable, as then $\mathbb{A}$ is a countable union of finite sets, so by Theorem 6, is countable.
In fact, it suffices to show that for each $d \in \mathbb{N}$, the set P_d of all integer polynomials of

degree d is countable, again by Theorem 6.
But the map $P_d \to \mathbb{Z}^{d+1}$ by

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \mapsto (a_d, a_{d-1}, \ldots, a_1, a_0)$$

is an injection, so since $\mathbb{Z}^{d+1}$ is countable, P_d is countable. □

A set is *uncountable* if it is not countable. Do uncountable sets exists?

Theorem 8. $\mathbb{R}$ is uncountable.

Proof. If $\mathbb{R}$ were countable, we would be able to list all the reals as $r_1, r_2, r_3, \ldots$. Write each r_n in decimal form in some way.

$$\begin{aligned} r_1 &= n_1.d_{11}d_{12}d_{13}d_{14}\ldots \\ r_2 &= n_2.d_{21}d_{22}d_{23}d_{24}\ldots \\ r_3 &= n_3.d_{31}d_{32}d_{33}d_{34}\ldots \\ &\vdots \end{aligned}$$

Define $r = 0.d_1d_2d_3\ldots$ by

$$d_n = \begin{cases} 1 & \text{if } d_{nn} \neq 1 \\ 2 & \text{if } d_{nn} = 1 \end{cases}$$

This r has only one decimal expansion and is not on the list (because $\forall\, n \in \mathbb{N}$, $r \neq r_n$). This contradicts the assumption that $\mathbb{R}$ is countable. □
This is known as a “diagonal argument”, due to Cantor (1875). Note that it in fact shows that $(0, 1)$ is uncountable.

Corollary 9. There are uncountably many transcendental numbers.

Proof. If $\mathbb{R} \setminus \mathbb{A}$ were countable, then since $\mathbb{A}$ is countable, $\mathbb{R} = \mathbb{R} \setminus \mathbb{A} \cup \mathbb{A}$ would be countable. ⨳ □

Theorem 10. $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof 1. If $\mathcal{P}(\mathbb{N})$ were countable, we could list the subsets of $\mathbb{N}$ as $S_1, S_2, S_3, \ldots$. Let $S = \{n \in \mathbb{N} : n \notin S_n\}$. Then S is not on our list since $\forall\, n \in \mathbb{N}$, $S \neq S_n$ (as S and S_n differ in their membership of the element n). ⨳ Hence $\mathcal{P}(\mathbb{N})$ is uncountable. □

Note that this is again a “diagonal argument”.
Proof 2. Note that there is an injection from $(0, 1)$ into $\mathcal{P}(\mathbb{N})$: write $x \in (0, 1)$ in binary $0.x_1x_2x_3$ with $x_i \in \{0, 1\}$ (not ending in an infinite string of 1s) and set $f(x) = \{n : n : x_n = 1\}$, for example

$$0.11101000\cdots \mapsto \{1, 2, 3, 5\}.$$

This is an injection. □

In fact, Proof 1 of Theorem 10 shows that following.

Theorem 11. For any set X, there is no bijection between X and $\mathcal{P}(X)$.

Proof. Given any function $f : X \to \mathcal{P}(X)$, we shall show that f is not a surjection. Indeed, let

$$S = \{x \in X : x \notin f(x)\}.$$

Then S does not belong to the image of f, since $\forall\, x \in X$, S and $f(x)$ differ in the element x, and thus $S \neq f(x)$. □

Remarks

(1) This is reminiscent of Russell's Paradox.

(2) In fact, it gives another proof that there is no universal set. For suppose we had such a universal set V, then we would have $\mathcal{P}(V) \subseteq V$, in which case there would certainly be a surjection from V to $\mathcal{P}(V)$.

Example. Let $\{A_i : i \in I\}$ be a family of open intervals of $\mathbb{R}$ which are pairwise disjoint. Must the family be countable? Note we can't simply count them from left to right; there isn't necessarily a clear choice for the "next" interval, and there is no guarantee that we will count all of them. The family $\{A_i : i \in I\}$ is nevertheless countable.

Proof 1. Each interval A_i contains a rational, and $\mathbb{Q}$ is countable, so since the intervals are disjoint, we have an injection from I into $\mathbb{Q}$. Hence the family $\{A_i : i \in I\}$ is countable. □

Proof 2. The set $\{i \in I : A_i \text{ has length } \geq 1\}$ is countable as it injects into $\mathbb{Z}$. Similarly, the set $\{i \in I : A_i \text{ has length } \geq \frac{1}{2}\}$ is countable as it injects into $\frac{1}{2}\mathbb{Z}$. More generally, for each $n \in \mathbb{N}$, $\{i \in I : A_i \text{ has length } \geq \frac{1}{n}\}$ is countable. Now $\{A_i : i \in I\}$ is countable as it is a countable union of countable sets. □

Summary

To show that X is uncountable

(1) Run a diagonal argument on X;

(2) Inject your favourite uncountable set into X.

To show that X is countable:

(1) list it (may be fiddly);

(2) inject it into $\mathbb{N}$;

(3) use "countable unions of countable sets are countable";

(4) if "in/near" $\mathbb{R}$, consider $\mathbb{Q}$.

Intuitively, we think of "A bijects with B" as saying that "A and B are of the same size", "A injects into B" as saying that "A is at most as big as B", and "A surjects onto B" as saying that "A is at least as big as B" (for $B \neq \emptyset$). For these interpretations to make sense, we need that if "A is at most as big as B", then "B is at least as big as A", and conversely.

Lemma 12. Given non-empty sets A and B, $\exists$ injection$f : A \to B \iff \exists$ surjection$g : B \to A$.

Proof. Suppose $f : A \to B$ is injective. Fix $a_0 \in A$. Define

$$g : B \to A, \qquad b \mapsto \begin{cases} \text{unique } a \in A \text{ such that } f(a) = b & \text{if it exists} \\ a_0 & \text{otherwise} \end{cases}$$

Then g is surjective.
Conversely, suppose $g : B \to A$ is surjective. Define

$$f : A \to B, \qquad a \mapsto \text{some } b \in B \text{ such that } g(b) = a.$$

Then f is injective. □

Theorem 13 (Schröder-Bernstein Theorem)**.** 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 $b \in B$, write $f^{-1}(b)$ for the $a \in A$ (if it exists) such that $f(a) = b$.
We call $g^{-1}(a), f^{-1}(g^{-1}(a)), g^{-1}(f^{-1}(g^{-1}(a))), \ldots$ the ancestor sequence of $a \in A$ (might terminate). Similarly, we can determine the ancestor sequence of $b \in B$. Define

$$\begin{aligned} A_0 &= \{a \in A : \text{ancestor sequence of } a \text{ stops at an even time, i.e. last point is in } A.\} \\ A_1 &= \{a \in A : \text{ancestor sequence of } a \text{ stops at an even time, i.e. last point is in } B\} \\ A_\infty &= \{a \in A : \text{ancestor sequence does not stop}\} \end{aligned}$$

Similarly, define B_0, B_1, B_∞. Note that f bijects A_0 with B_1 (observing that every $b \in B$ has at least one ancestor, so is $f(a)$ for some $a \in A_0$), and similarly, g bijects B_0 with A_1. And f (or g) biject A_∞ with B_∞. Then the function $h : A \to B$ defined as

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

is a bijection. □

This means that we have that if "A is at most as big as B" and "B is at most as big as A", then "A is of the same size as B".

Example. Is there a bijection from $[0,1]$ to $[0,1] \cup [2,3]$?
Observe we have an injection $f : [0,1] \to [0,1] \cup [2,3]$ by using $x \mapsto x$ and an injection $g : [0,1] \cup [2,3] \to [0,1]$ using $x \mapsto \frac{x}{3}$, so by Schröder-Bernstein there is a bijection between $[0,1]$ and $[0,1] \cup [2,3]$.

It would also be nice to be able to say that for any two sets A and B, either A injects into B or B injects into A. This is true, but harder to prove (see Part II Logic & Set Theory).

Question Does every set X inject into one of

$$\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \ldots?$$

No, for example consider

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

Does every set X' inject into one of

$$X, \mathcal{P}(X), \mathcal{P}(\mathcal{P}(X)), \mathcal{P}(\mathcal{P}(\mathcal{P}(X))), \ldots?$$

No, for example consider

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

Does every set X'' inject into one of

$$X', \mathcal{P}(X'), \mathcal{P}(\mathcal{P}(X')), \mathcal{P}(\mathcal{P}(\mathcal{P}(X'))), \ldots?$$

No, for example consider

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

Does every set Y inject into one of $X, X', X'', \ldots$?
No, for example

$$Y = X \cup X' \cup X'' \cup \cdots$$

Panorama

- II Logic & Set Theory
- IA Analysis
- IB Groups, Rings and Modules
- II Number Theory

Chapter V: More about primes (non-examinable)

Bertrand postulated in 1845 that for every $n \in \mathbb{N}$, there is always a prime between n and $2n$, i.e. $n \le p < 2n$. The primes 2, 5, 11, 23, 47, 89, 179, 359, 719, 1439, 2879 show it to be true for $n \le 2^{11}$. Bertrand checked it for $n < 3,000,000$. Chebychev (1850) gave a proof. Erdös (1932) have an elementary proof based on the properties of $\binom{2n}{n}$.

Observation 1.

$$\binom{2n}{n} \ge \frac{2^{2n}}{2n+1}$$

Proof. Since

$$\frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{n-k}{k+1},$$

it is evident that $\binom{n}{k}$ increases for $k < \frac{n}{2}$, and decreases for $k > \frac{n}{2}$. In particular, $\binom{2n}{n}$ is the largest binomial coefficient, so

$$\binom{2n}{n} \ge \frac{\sum_{k=0}^{2n} \binom{2n}{k}}{2n+1} = \frac{2^{2n}}{2n+1}$$

□

Observation 2. If $p \le n$ is a prime dividing $\binom{2n}{n}$, then $p \le \frac{2n}{3}$.

Proof. Suppose $\frac{2n}{3} < p \le n$, then

$$p \le n < 2p \le 2n < 3p$$

so the numerator and denominator of

$$\frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 3 \cdot 2 \cdot 1}$$

are divisible by exactly one copy of p. *Correction: this is only true assuming* $p > 3$ *or* $n > 3$, *in order to make sure we don't get any multiples of* p^2. ⨳ □

Observation 3. If p is a prime and $p^k \mid \binom{2n}{n}$, then $p^k \le 2n$.

Proof. The greatest power of p dividing $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$.

$$\underbrace{\left\lfloor \frac{n}{p} \right\rfloor}_{\substack{\text{multiples of} \\ p \le n}} + \underbrace{\left\lfloor \frac{n}{p^2} \right\rfloor}_{\substack{\text{multiples of} \\ p^2 \le n}} + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \sum_{i \ge 1} \frac{n}{p^i}$$

Hence, if k is a power of p dividing $\binom{2n}{n} = \frac{2n!}{(n!)^2}$, then

$$\begin{aligned}
k &= \sum_{i\geq 1} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\sum_{i\geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{l} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) && \text{where } l \text{ is the greatest power of } p \text{ such that } p^l \leq 2n. \\
&\leq \sum_{i=1}^{l} 1 && \text{since } \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1 \\
&= l
\end{aligned}$$

so $k \leq l$ and thus $p^k \leq p^l < 2n$. □

Observation 4. For all $m \in \mathbb{N}$,

$$\prod_{\substack{p\leq m \\ p \text{ prime}}} p \leq 4^m.$$

Proof. By induction on m. True for $m = 2$. If $m > 2$ is even, then

$$\prod_{p\leq m} p = \prod_{p\leq m-1} p \leq 4^{m-1} < 4^m.$$

If $m = 2k+1$ is odd, then all primes $k+2 \leq p \leq 2k+1$ divide

$$\binom{2k+1}{k} = \frac{(2k+1)!}{k!(k+1)!} = \frac{(2k+1)\cdot 2k \cdots (k+2)}{k\cdot (k-1)\cdots 3\cdot 2\cdot 1}$$

Thus,

$$\prod_{k+2\leq p\leq 2k+1} p \leq \binom{2k+1}{k} = \binom{2k+1}{k+1} \leq \frac{2^{2k+1}}{2} = 4^k.$$

By the inductive hypothesis,

$$\prod_{p=m} p = \prod_{p\leq k+1} p \cdot \prod_{k+2\leq p\leq 2k+1} p \leq 4^{k+1}\cdot 4^k = 4^{2k+1}.$$

□

Theorem 5 (Bertrand's Postulate)**.** For all $n \in \mathbb{N}$, there exists a prime p with $n \leq p < 2n$.

Proof. Clearly the primes factors of $\binom{2n}{n}$ are all less than $2n$ (assuming $n > 1$ so that $2n$ is not prime). Suppose the theorem fails. Then all prime factors of $\binom{2n}{n}$ are in fact less than n. But by Observation 2, they are all less than $\frac{2n}{3}$. Consider the prime factorisation of $\binom{2n}{n}$. By Observation 3, each prime contributes at most $2n$ to the factorisation. Moreover, if $p > \sqrt{2n}$, then p contributes at most p to the factorisation (since $p^2 > 2n$). Now by Observation 1 and the above

$$\begin{aligned}\frac{2^{2n}}{2n+1} &\le \binom{2n}{n} \\ &\le \prod_{p\le\sqrt{2n}} 2n \prod_{\sqrt{2n}<p\le 2n/3} p \\ &\le (2n)^{\sqrt{2n}} \cdot \prod_{p<2n/3} p\end{aligned}$$

But by Observation 4,

$$\prod_{p<2n/3} p \le 4^{2n/3}.$$

so

$$\frac{4^n}{2n+1} \le (2n)^{\sqrt{2n}} \cdot 4^{2n/3},$$

Which fails when n is large. How large? This is equivalent to

$$4^{n/3} \le (2n+1)(2n)^{\sqrt{2n}}$$

and $2n+1 \le (2n)^2 \le (2n)^{\sqrt{2n}/3}$ for $n \ge 18$. So

$$4^{n/3} \le (2n)^{4\sqrt{2n}/3}$$

or

$$4^n \le (2n)^{4\sqrt{2n}}$$

With $r = \sqrt{2n}$, this is

$$4^{r^2/2} \le r^{8r}$$

or

$$4^r \le r^{16}$$

which fails when $r = 2^6 = 64$ and larger. So proof holds when $n \ge 2^{11}$, and also true for smaller values of n. □