Numbers and Sets - Lecture 1

8/10/20

Chapter 1 - elementary NT
Chapter 2 - the reals
Chapter 3 - sets and functions
Chapter 4 - countability

4 example sheets per course

(here $\mathbb{N}$ is positive integers)

Chapter 0 - proof

A proof is a logical argument that establishes a conclusion.

Prove things 1) to be sure they're true
2) to understand why they're true

Examples of proofs and non-proofs

1. Claim $n^3 - n$ is always a multiple of 3 for $n \in \mathbb{N}$.

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

   (product of 3 consecutive numbers)

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

   So $(n-1)n(n+1)$ is a multiple of 3. □

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

   (Non) Proof Given $n \in \mathbb{N}$ that is even, we have $n = 2k$, $k \in \mathbb{N}$.

   So $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ so n^2 is even. □

   This is a wrong proof: wrong way round

   "if A then B" is not the same as "if B then A"

3. Claim For any $n \in \mathbb{N}$, if n^2 is a multiple of 9 then so is n.

   (Non) Proof For any $n \in \mathbb{N}$ that's a multiple of 9, $n = 9k$ for some $k \in \mathbb{N}$. So $n^2 = 81k^2 = 9(9k^2)$,

   so n^2 is a multiple of 9. □

   But this time the claim isn't even true.

To show "if A then B" is false, it's sufficient to find one counterexample where A is true and B is false.

Back to "if n^2 is even then n is even"

Proof "Suppose n^2 is even. Then for some $k \in \mathbb{N}$, $n^2 = 2k$."

This statement may be harder to work with e.g. $n = \sqrt{2}\sqrt{k}$ isn't as easy to work with.

So suppose that n is odd. So $n = 2k+1$ for some $k \in \mathbb{N}_0$.

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

which is odd. # "contradiction"

Thus n is even. □

Note the claim was true because of properties of odd numbers.

To show "if A then B" we showed that there is no case where A is true and B is false.

Another viewpoint: To show $A \Rightarrow B$ (A implies B)

This is the same as NOT B $\Rightarrow$ NOT A

Numbers and Sets - Lecture 2

10/10/20

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

This is really 2 assertions: 1) $x = 2$ and $x = 3$ are solutions of $x^2 - 5x + 6 = 0$

2) there are no other solutions.

Equivalently 1) $x = 2$ or $x = 3 \Rightarrow x^2 - 5x + 6 = 0$

2) $x^2 - 5x + 6 = 0 \Rightarrow x = 2$ or $x = 3$

so claim is $x = 2$ or $x = 3 \iff x^2 - 5x + 6 = 0$.

Proof If $x = 2$ or $x = 3$

then $x - 2 = 0$ or $x - 3 = 0$

so $(x-2)(x-3) = 0$ so $x^2 - 5x + 6 = 0$. ✓

If $x^2 - 5x + 6 = 0$ then $(x-2)(x-3) = 0$

so $x - 2$ is 0 or $x - 3$ is 0

so $x = 2$ or $x = 3$ ✓ □

Alternative Proof For any real x,

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

$\iff x - 2 = 0$ or $x - 3 = 0$

$\iff x = 2$ or $x = 3$. □

Claim Every positive real number is at least 1.

(Non)-Proof Let x be the smallest positive real - then we try to show it's 1.

Suppose for contradiction that $x \neq 1$. Then $x < 1$ or $x > 1$.

If $x < 1$: $0 < x^2 < x$ which is impossible as it contradicts the definition that x is the smallest positive real. ✳

If $x > 1$ then $\sqrt{x} < x$ contradicting definition. ✳

So $x = 1$. □

The "proof" assumes that there is a smallest positive real. This is nonsense, so so are the statements that follow from this assumption.

Moral: Every line in a proof must be justified.

Chapter 1 : Elementary Number Theory

Intuitively, the natural numbers (written $\mathbb{N}$) consist of

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

↑ How to make precise?

What we assume The natural numbers ($\mathbb{N}$) is a set containing an element "1" and an operation "+1" satisfying

1) For all n, $n+1 \neq 1$
2) If $m \neq n$ then $m+1 \neq n+1$

} capture "all on list are different"

3) For any property $p(n)$: if $p(1)$ is true and for every n, if $p(n)$ is true then $p(n+1)$ is true, then $p(n)$ is true for all n. "induction axiom"

(These 3 are the Peano axioms.

To see why 3) captures our intuitive notion of "that list is everything" we can use induction – take $p(n)$ = "n is on the list".

Can write 2 for $1+1$ and have operation "+2" defined by $n+2 = (n+1)+1$

In fact we can define "$+k$" for any $k \in \mathbb{N}$ by:

$n + (k+1) = (n+k) + 1$ for each $n \in \mathbb{N}$

By induction this defines $n+k$ (with operation "$+k$")

Take $p(k) =$ "$+k$ is defined".

$+1$ is defined.

If $+k$ is defined, then using $(n+k)+1 = n+(k+1)$ we have $k+1$ is defined. □

Similarly we can define multiplication, powers, etc.

Can check the usual rules of arithmetic:

1) $\forall a, b \quad a+b = b+a$ ($+$ is commutative)

2) $\forall a, b \quad ab = ba$ ($\times$ is commutative)

3) $\forall a, b, c \quad a+(b+c) = (a+b)+c$ ($+$ is associative)

4) $\forall a, b, c \quad a(bc) = (ab)c$ ($\times$ is associative)

5) $\forall a, b, c \quad a(b+c) = (ab)+(ac)$ ($\times$ is distributive over $+$)

Define $a < b$ if $a+c = b$ for some $c \in \mathbb{N}$ (no 0).

6) $\forall a, b$: if $a < b$ then $a+c < b+c$

7) $\forall a, b$: $a < b \Rightarrow ac < bc$

8) $\forall a, b, c$: $a < b$, $b < c \Rightarrow a < c$

9) $\forall a$: NOT $a < a$

A more useful form of induction:

Induction says that if $P(1)$ and $\forall n$, $P(n) \Rightarrow P(n+1)$ then $P(n)$ $\forall n$.

Strong induction: if $P(1)$ and $\forall n$ we have $P(m)\ \forall m \leq n \Rightarrow P(n+1)$ then $P(n)$ $\forall n$.

To deduce this from ordinary induction, apply ordinary induction to $Q(n)$ where $Q(n)$ is "$P(m)\ \forall m \leq n$".

Remarks: 1) Technically you don't need to check $n=1$ case separately (as implied by the condition if interpreted suitably) – technically none are false below $n=1$ (but always check anyway)

correct view of induction – really works "down", not "up" → 2) Normally to prove $P(n)$ $\forall n$ we take n and show $P(n)$. Strong induction allows you to assume it's true for smaller cases if it helps (e.g. $P(m)$ for $m<n$).

2 equivalent forms of strong induction

1. If $P(n)$ is false for some n then for some n we must have $P(n)$ false but $P(m)$ true $\forall m \leq n$.

   "If there is a counterexample, then there is a minimal counterexample"

2. If $P(n)$ is true for some n then there is a least n with $P(n)$.

   "Well-ordering principle"

   (There's something else unrelated called the well-ordering theorem)

The Integers

The integers, written $\mathbb{Z}$, consist of all symbols $n, -n$ (n a natural number) and 0.

Can define $+$, $\times$ etc on $\mathbb{Z}$ from $\mathbb{N}$.

We can check all the previous algebraic rules, plus

$\forall a \quad a+0 = a$ (identity for $+$)

$\forall a \; \exists b \quad$ s.t. $\quad a+b = 0$ (inverses for $+$)

Define $a < b$ if $\exists\, c \in \mathbb{N}$ with $a+c = b$.

All previous rules still hold except one change

$\forall a, b, c$: If $a < b$, $\underline{c > 0}$ then $ac < bc$

The Rationals

The rationals, written $\mathbb{Q}$, consist of all expressions $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$, with $\frac{a}{b}$ regarded as the same as $\frac{c}{d}$ if $ad = bc$.

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (can check: does not matter how $\frac{a}{b}, \frac{c}{d}$ written to be well defined).

Note cannot define operation on $\mathbb{Q}$ by

$$\frac{a}{b} \mapsto \frac{a^2}{b^3} \quad \text{as e.g.} \quad \frac{1}{2} \mapsto \frac{1}{8}$$

$$\frac{2}{4} \mapsto \frac{4}{64} = \frac{1}{16} \neq \frac{1}{8}$$

Similarly can check algebraic rules. Also

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

Define $\frac{a}{c} \times \frac{b}{d}$ (where $c, d \neq 0$)

Define $\frac{a}{b} < \frac{c}{d}$ (where $b, d > 0$) if $ad < bc$.

(can check $\mathbb{Z}$ rules hold).

Note: Can view $\mathbb{Z}$ as "living inside" $\mathbb{Q}$ by identifying $a \in \mathbb{Z}$ with $\frac{a}{1}$ in $\mathbb{Q}$

Structure of $\mathbb{N}$ under $+$ is easy: start at 1, keep doing $+1$.
What about under $\cdot$?
↑ (meaning multiplication, $\times$)

Primes (not definition) For $n \in \mathbb{N}$, the multiples of n are all integers kn for some $k \in \mathbb{Z}$. e.g. $2n, 3n, 16n, n, -5n, 0$

If m is a multiple of n, say n divides m or
n is a divisor / factor of m
or $n \mid m$.

Definition (Prime) A natural number $n \geq 2$ is prime if its only divisors are $1, n$.

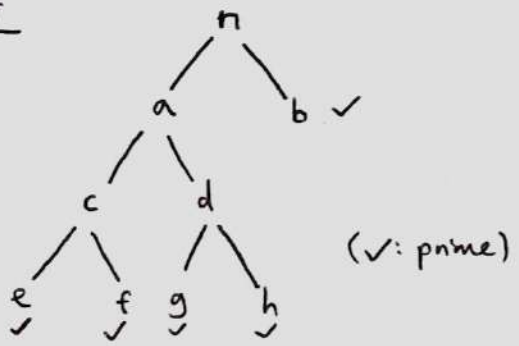
(We don't allow 1 to be prime, otherwise e.g. $15 = 3\times5, 1\times3\times5, 1^2\times3\times5, \ldots$)

If $n \geq 2$ is not prime, then it is composite.

Aim: "Break up" any number into a unique product of primes.
e.g. $63 = 3\times3\times7$

Proposition 1 Every natural number with $n \geq 2$ is expressible as a product of primes.

Proof



This will eventually terminate
This may be hard to write out as a proper proof so use induction.

Induction on n: $n = 2$ ✓

Given $n > 2$:

If n is prime ✓

If not (n is composite), then $n = ab$, for some $1 < a, b < n$

By induction hypothesis we've assumed that

$a = p_1 p_2 p_3 \cdots p_k$, $b = q_1 q_2 q_3 \cdots q_l$ for p_i, q_i prime

Then $n = p_1 p_2 p_3 \cdots p_k q_1 q_2 q_3 \cdots q_l$, a product of primes.

✓ □

Remark Can define an empty product (i.e. of no primes) to be 1.

If so, then Proposition 1 could start $n \geq 1$.

Theorem There are infinitely many primes.

Proof Suppose there are finitely many primes $p_1, p_2, \dots, p_k$.

All p_i divide $p_1 p_2 \dots p_k$ so none divide $p_1 p_2 \dots p_k + 1 = n$.

So n has no prime factor. ⁂ □

There is no formula for the n^{th} prime.

Want: Prime factorisation of a number is unique (up to reordering)

We need $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ for p prime

Highest Common Factors

For $a, b \in \mathbb{N}$, we have $c \in \mathbb{N}$ is the HCF of a and b if $c \mid a$, $c \mid b$ and if $d \mid a$, $d \mid b$ then $d \mid c$.

("c is a common factor of a and b, and every common factor divides c")

e.g. 18 and 12: 18's factors 1, 2, 3, 6, 9, 18

12's factors 1, 2, 3, 4, 6, 12

Common factors are 1, 2, 3, 6

So the HCF (if it exists) is the greatest of all common factors but if a and b had common factors 1, 2, 3, 4, 6 then a and b would not have a HCF.

Aim show that $\forall a, b$, HCF (a, b) exists.

PTO

Proposition 3 (Division Algorithm) Let $n, k \in \mathbb{N}$. Then we can write $n = qk + r$ where $q, r \in \mathbb{Z}$ with $0 \leq r \leq k-1$.

Proof Induction on n: $n = 1 = 0k + 1$ ✓

Given $n > 1$:

Have $n-1 = qk + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r \leq k-1$.

If $r < k-1$ then $n = qk + (r+1)$ ✓

If $r = k-1$ then $n = (q+1)k$ ✓ ✓ □

Euclid's Algorithm For finding hcf (a, b) (say $a \geq b$)

This proves hcf exists and gives a quick way to find it.

Algorithm

Write $a = q_1 b + r_1$ $(q_i, r_i \in \mathbb{Z}, 0 \leq r_i < b)$

Write $b = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

...

Continue until you get

$r_{n-1} = q_{n+1} r_n + r_{n+1}$ with

$r_{n+1} = 0$

Then hcf is r_n.

Example

$a = 372$, $b = 162$

$372 = 2 \times 162 + 48$

repeat:

$162 = 3 \times 48 + 18$

$48 = 2 \times 18 + 12$

$18 = 1 \times 12 + 6$

$12 = 2 \times 6$

output 6

Note: terminates because numbers decrease

Terminates in $\leq b$ steps since $b > r_1 > r_2 > \ldots$

so we must get a "hcf". It must exist.

We then show that this "hcf" satisfies the required properties:

Theorem 4 The output of the algorithm on a, b is $\text{hcf}(a, b)$.

Proof (i) $r_n \mid r_{n-1}$ (as $r_{n+1} = 0$), from the last line

so $r_n \mid r_{n-2}$ (by 2nd last line)

so $r_n \mid r_i \ \forall i$ inductively.

So $r_n \mid b$ (2nd line)

so $r_n \mid a$. So r_n is a common factor.

(ii) Given d with $d \mid a$, $d \mid b$:

We have $d \mid r_1$ (1st line)

so $d \mid r_2$ (2nd line)

and inductively $d \mid r_i \ \forall i$

so $d \mid r_n$ as required. □

e.g. HCF of 87, 52 - use Euclid's algorithm.

(1) $87 = 1 \times 52 + 35$
(2) $52 = 1 \times 35 + 17$
(3) $35 = 2 \times 17 + 1$
(4) $17 = 17 \times 1$

$87 = 3 \times 29$
$52 = 2^2 \times 13$

$\text{hcf}(87, 52) = 1$

We have that $\text{hcf}(87, 52) = 1$ or write as $(87, 52) = 1$ (coprime)

Can we write 1 as a multiple of 87 + a multiple of 52?

$87x + 52y = 1$ for some $x, y \in \mathbb{Z}$

Lecture 5 page 1/4

We have $1 = 1 \times 35 - 2 \times 17$ from (3)

$\Rightarrow 1 = 1 \times 35 - 2(52 - 35)$ from (2)

$\Rightarrow 1 = -2 \times 52 + 3 \times 35$

$\Rightarrow 1 = -2 \times 52 + 3(87 - 52)$ from (1)

$\Rightarrow 1 = 3 \times 87 - 5 \times 52$

so we have a solution $x = 3, \; y = -5$.

Theorem 5 $\forall a, b \in \mathbb{N} \;\; \exists x, y \in \mathbb{Z}$ such that $ax + by = \text{hcf}(a, b)$
"can write hcf as a linear combination of a and b"

Proof 1 Run Euclid on a and b, say with output r_n.

Have $r_n = x r_{n-1} + y r_{n-2}$ (from 2nd last line of alg.)
$r_{n-2} = q_n r_{n-1} + r_n$

But r_{n-1} is expressible as $x r_{n-2} + y r_{n-3}$, $x, y \in \mathbb{Z}$ (3rd last line)

then substitute for r_n

$r_n = x r_{n-2} + y r_{n-3}$

(note x, y not the same from line to line)

Continue: we obtain that $\forall i : r_n = x r_i + y r_{i-1}$, $x, y \in \mathbb{Z}$ (inductively)

So $r_n = ax + by$ for some $x, y \in \mathbb{Z}$ (from line 1 of Euclid). □

Note: Euclid is showing x, y exist and how to get them.

Proof 2 Let h be the least positive linear combination of a and b.

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

Proof (ii) Given $d|a$, $d|b$, $d|xa+yb$ $\forall x,y \in \mathbb{Z}$
so $d|h$.

(i) Suppose $h \nmid a$. Then $a = qh+r$, $q, r \in \mathbb{Z}$ and $0 < r < h$.

Then $r = a - qh = a - q(xa+yb)$, also a linear combination. But $r < h$ and h is the least positive LC. ✱

so $h|a$ and similarly $h|b$. □

Lecture 5 page 2/4

This doesn't show how to find x, y though.

Application: Solving integer linear equations

Suppose $a, b \in \mathbb{N}$. When can we solve

$ax = b$, $\quad x \in \mathbb{Z}$?

If $x \in \mathbb{Q}$ allowed, then always

Otherwise, it's iff $a|b$.

Now consider $ax + by = c \quad x, y \in \mathbb{Z}$

e.g. $320x + 72y = 33$ not possible: LHS even RHS odd

$87x + 52y = 33$?

Possible: $87x + 52y = 1$ has a solution so just multiply by 33. ✱

Corollary 6 Let $a, b, c \in \mathbb{N}$. Then $ax + by = c$ has an integer solution iff $hcf(a, b) \mid c$.

Proof Let $h = hcf(a, b)$.

$\Rightarrow$ Have $ax + by = c$ for $x, y \in \mathbb{Z}$

But $h \mid a$, $h \mid b$ so $h \mid ax + by$.

$\Leftarrow$ Have $h = ax + by$ for some $x, y \in \mathbb{Z}$

Multiply up by $\frac{c}{h}$ (we know $h \mid c$ so $\frac{c}{h} \in \mathbb{Z}$) :.

$c = a\left(\frac{xc}{h}\right) + b\left(\frac{yc}{h}\right)$ giving a solution. □

Remark Corollary 6 is ~~something~~ sometimes called Bezout's theorem.

Lemma 7 Let p be prime and $a, b \in \mathbb{N}$.

Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Proof Suppose $p \nmid a$ then we want to show $p \mid b$.

Then $hcf(p, a) = 1$. (p prime)

So $px + ay = 1$, $x, y \in \mathbb{Z}$.

Then $pbx + aby = b$,

where b is a multiple of p because

$p \mid pbx$ and $p \mid ab$ so ~~$pbx + aby$~~ $p \mid pbx + aby$

$\Rightarrow p \mid b$. □

Remarks

1) Similarly $p \mid a_1 a_2 \ldots a_n \Rightarrow p \mid a_i$ for some i. (Inductively)

2) We need p to be prime.

Theorem 8 (Fundamental Theorem of Arithmetic)

Every number $n \in \mathbb{N}$ $(n \geq 2)$ is expressible as a product of primes, uniquely up to reordering.

Proof **Existence**: Proposition 1 proved this ✓ (lecture 3)

Uniqueness: Induction on n: $n = 2$ ✓

Given $n > 2$: Suppose $n = p_1 \dots p_k = q_1 \dots q_l$ where p_i, q_i are prime. Must show $k = l$ and after reordering, $p_i = q_i \ \forall i$.

We have $p_1 \mid n \Rightarrow p_1 \mid q_1 \dots q_l \Rightarrow p_1 \mid q_i$ for some i.

Reorder to assume $p_1 \mid q_1$.

(†) But q_1 is prime, so $p_1 = q_1$.

(*) Then $\frac{n}{p_1} = p_2 \dots p_k = q_2 \dots q_l$. Repeat argument (inductively)

Thus $k = l$ and $p_2 = q_2, p_3 = q_3, \dots, p_k = q_k$ (induction). □

Remark This argument works: we've checked it's true for $n = 2$. Although line (*) is written below, we can think of it as assuming the uniqueness property holds for all values less than n so true for $\frac{n}{p_1}$.

Then write $n = p_1 \dots p_k = q_1 \dots q_l$ and have $p_1 = q_1$.

More straightforward way: Once we get to line (†) we divide by p_1 to give (*). Then we can repeat the same argument with $\frac{n}{p_1}$ instead of n. So it works as a kind of "downwards" inductive proof.

Numbers and Sets – Lecture 6

20/10/20

Digression In FTA we took the "things that cannot be broken up" (primes) and broke up every number as a product of these uniquely.

Consider $\mathbb{Z}[\sqrt{-3}] = a + b\sqrt{-3} = a + b\sqrt{3}\,i$ for $a, b \in \mathbb{Z}$.

Can add / multiply 2 such elements and get something of the same form.

So we can talk about "divides" / "multiple of" in $\mathbb{Z}[\sqrt{-3}]$

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

All these terms can't be broken up: "unique factorisation" fails in $\mathbb{Z}[\sqrt{-3}]$

FLT can be "proved" if unique factorisation is assumed in certain situations.

Applications of FTA

1) Factors

What are the factors of $2^3 \times 3^7 \times 11^n$?

All of the form $2^a 3^b 11^c$ $(0 \le a \le 3,\ 0 \le b \le 7,\ 0 \le c \le 1)$ $a, b, c \in \mathbb{Z}$

are factors. There are no others – if $7 \mid n$ then you'd have a factorisation involving 7. The factorisation must be unique so this is impossible.

So the factors of $n = p_1^{a_1} \dots p_k^{a_k}$ are precisely all numbers $p_1^{b_1} \dots p_k^{b_k}$ for $0 \le b_i \le a_i$.

2) HCFs

Common factors of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$

All $2^a 3^b 11^c$, $0 \le a \le 3$, $0 \le b \le 2$, $0 \le c \le 1$ are common factors: $2^3 3^2 11$ is HCF.

In general, HCF of $p_1^{a_1} \dots p_k^{a_k}$ and $p_1^{b_1} \dots p_k^{b_k}$ $(a_i, b_i \geq 0)$ is

$p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$

3) LCMs

Common multiples of $2^3 3^7 5\, 11^3$ and $2^4 3^2 11 \cdot 13$ are all $2^a \cdot 3^b \cdot 5^c \cdot 11^d \cdot 13^e \cdot$ (anything)

$a \geq 4,\ b \geq 7,\ c \geq 1,\ d \geq 3,\ e \geq 1$

so $2^4 \cdot 3^7 \cdot 5^a \cdot 11^3 \cdot 13$ is the LCM.

In general LCM of $p_1^{a_1} \dots p_k^{a_k}$ and $p_1^{b_1} \dots p_k^{b_k}$ $(a_i, b_i \geq 0)$ is

$p_1^{\max(a_1, b_1)} \dots p_k^{\max(a_k, b_k)}$.

Consequence: take $\text{hcf}(x, y)\, \text{lcm}(x, y) = xy$

(since $\min(a,b) + \max(a,b) = a+b$).

Modular Arithmetic

Let $n \geq 2$ be a natural number. The integers mod n ($\mathbb{Z}_n$) consist of the integers with two regarded as the same if they differ by a multiple of n.

e.g. in $\mathbb{Z}_7$ 2 is the same as 16.

If x, y are the same in $\mathbb{Z}_n$, can write $x \equiv y \pmod n$

$x \equiv y \ (n)$

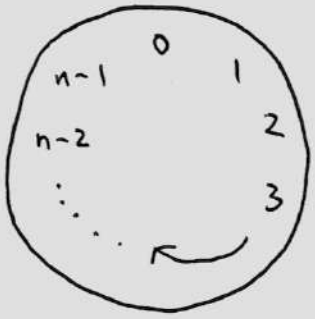
or $x = y$ in $\mathbb{Z}_n$

Thus $x \equiv y \bmod n \iff x - y$ is a multiple of n.

$\iff x = y + kn, \ k \in \mathbb{Z}$.

Note that no two of $0, 1, \ldots, n-1$ are congruent mod n and every x is congruent to one of them mod n (division algorithm)

Can view $\mathbb{Z}_n$ as



"correct picture" of $\mathbb{Z}_n$

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

(Note: even/odd do not make sense in general, e.g. $2 \equiv 9 \bmod 7$)

We want: if $a \equiv a'(n)$, $b \equiv b'(n) \Rightarrow a+b \equiv a'+b'(n)$
and $ab \equiv a'b'(n)$

Have $a' = a + kn \quad (k \in \mathbb{Z})$

$b' = b + jn \quad (j \in \mathbb{Z})$

$a'+b' = a+b+(k+j)n$ so $a'+b' \equiv a+b \bmod n$ ✓

$a'b' = (a+kn)(b+jn) = ab + n(aj+bk+kjn)$

$\Rightarrow ab \equiv ab \bmod n$ ✓

Laws of arithmetic are inherited from $\mathbb{Z}$.

e.g. $a+b \equiv b+a \bmod n$

Some things we have already done are expressible in terms of M.A.:
e.g. "$p|ab \Rightarrow p|a$ or $p|b$" is $ab \equiv 0 \bmod p \iff a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$.

Inverses

For $a, b \in \mathbb{Z}_n$, say b is an inverse of a if $ab \equiv 1 \bmod n$.

e.g. in $\mathbb{Z}_{10}$ inverse of 3 could be 7.

There is no inverse of 4: $1 \bmod 10$ must make it odd.

Note 1. If inverse exists, then it's unique mod n

Suppose in $\mathbb{Z}_n$, $ab = ac = 1$

Then $b(ab) = b(ac) \Rightarrow 1(b) = 1(c)$.

2) If a inverted in $\mathbb{Z}_n$: can write a^{-1} for inverse.

Important 1) Can "cancel" an invertible.

If a^{-1} exists (in $\mathbb{Z}_n$) then $ab \equiv ac \bmod n$

$\Rightarrow b \equiv c \bmod n$

2) In general you cannot cancel.

e.g. in $\mathbb{Z}_{10}$ $4 \times 5 = 2 \times 5$ (n)

$\not\Rightarrow 4 = 2$ (n)

$\mathbb{Z}_p$ is very "well behaved" for p prime.

Proposition 9 Let p be prime. Then every $a \not\equiv 0 \bmod p$ is invertible mod p.

[Equivalently in $\mathbb{Z}_p$, $a \neq 0 \Rightarrow \exists b : ab = 1$]

Proof 1 Have $(a, p) = 1$.

So $ax + py = 1$ for some $x, y \in \mathbb{Z}$.

That is $ax = 1 - py \Rightarrow \underline{ax \equiv 1 \bmod p}$ as required. □

Proof 2 In $\mathbb{Z}_p$ consider all multiples of a

$a \times 0,\ a \times 1,\ a \times 2,\ \ldots,\ a(p-1)$

We must show one is 1.

All the multiples of a are distinct in $\mathbb{Z}_p$ as

$ia = ja \Rightarrow (i-j)a = 0 \Rightarrow i - j \equiv 0 \ (p)$ or

$a \equiv 0 \ (p)$ but p is prime so $\underline{i = j}$.

There are p distinct multiples mod p, so one *must* be 1 mod p. □

What about *general* n?

Proposition 9' Let $n \geq 2$. Then a is invertible mod n iff a is coprime to n : $(a, n) = 1$.

Proof $(a, n) = 1 \iff ax + ny = 1$ for some $x, y \in \mathbb{Z}$.

$\iff ax = 1 - ny$

$\iff ax \equiv 1 \bmod n$ □

The *Euler ϕ-function* is defined for each $n \in \mathbb{N}$ by

$\phi(n)$ = number of x $(1 \leq x \leq n)$ with $(x, n) = 1$.

(same as number of invertibles mod n).

e.g. p prime: $\phi(p) = p-1$

$\phi(p^2) = p^2 - p$ ($-p$ from $p, 2p, 3p, \dots, pp$)

p, q distinct primes: $\phi(pq) = pq - p - q + 1$

($-p$: multiples of q; $-q$: multiples of q; $+1$: from pq)

How do powers behave in $\mathbb{Z}_p$?

e.g. powers of 2 in $\mathbb{Z}_7$: $2^1 = 2$, $2^2 = 4$, $2^3 = 1$

(so it keeps repeating $2, 4, 1, 2, 4, 1, \dots$)

Note $2^6 \equiv 1 \bmod 7$.

Powers of 2 in $\mathbb{Z}_{11}$:

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$,

$2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$

Then repeats as we've got back to 1.

Theorem 10 (Fermat's Little Theorem) Let p be prime.

Then in $\mathbb{Z}_p$ (mod p), $a^{p-1} \equiv 1 \bmod p$ $\forall a \neq 0$.

Proof In $\mathbb{Z}_p$ consider $a \times 1, a \times 2, \dots, a \times (p-1)$

They are distinct in $\mathbb{Z}_p$ ($ai = aj \Rightarrow i = j$ as a is invertible).

And they are nonzero. $ai = 0 \Rightarrow a = 0$ or $i = 0$ ✱

They hence are $1, 2, \dots, p-1$ in some order.

Multiply them all: $a^{p-1}(p-1)! = (p-1)!$ in $\mathbb{Z}_p$

$(p-1)!$ is invertible as its factors all are, so

$a^{p-1} \equiv 1 \bmod p$ □

What about for general n?

Theorem 10' (Fermat – Euler theorem)

Let $n \geq 2$. Then in $\mathbb{Z}_n$, every invertible a has $a^{\phi(n)} = 1$.

Proof Let the units in $\mathbb{Z}_n$ be $x_1, x_2, \ldots, x_{\phi(n)}$.
(↑ word for invertibles)

Consider $ax_1, ax_2, \ldots, ax_{\phi(n)}$: all distinct

($ax_i = ax_j \Rightarrow x_i = x_j$ as a invertible)

and invertible.

So they are all the invertibles $x_1, x_2, \ldots, x_{\phi(n)}$ in some order.

Multiply them:

$$a^{\phi(n)} x_1 x_2 \ldots x_{\phi(n)} = \underbrace{x_1 x_2 \ldots x_{\phi(n)}}_{\text{invertible}}$$

$\Rightarrow$ $a^{\phi(n)} = 1$ in $\mathbb{Z}_n$. □

Question We know $(p-1)! \not\equiv 0 (p)$. What is it?

e.g. $p = 5$: $4! = 24 \equiv -1 (5)$

$p = 7$: $6! = 720 \equiv -1 (7)$

Lemma 11 Let p be prime. Then in $\mathbb{Z}_p$, $x^2 = 1$ $\Rightarrow$ $x = 1$ or $x = -1$.

Proof Work in $\mathbb{Z}_p$. $x^2 = 1 \Rightarrow x^2 - 1 = 0$

$\Rightarrow (x-1)(x+1) = 0$

$(x-1)(x+1) \equiv 0 \bmod p \Rightarrow x - 1 \equiv 0$ or $x + 1 \equiv 0$

$\Rightarrow x = \pm 1$. □

Remark Turns out that a nonzero polynomial of degree k in $\mathbb{Z}_p$ always has at most k roots in $\mathbb{Z}_p$.

Theorem 12 (Wilson's Theorem) Let p be prime. Then $(p-1)! \equiv -1 \bmod p$.

Proof May assume $p > 2$ (as obviously true for $p = 2$).

In $\mathbb{Z}_p$ consider $1, 2, 3, \ldots, p-1$.

Can pair up each a with its inverse a^{-1} (for $a \neq a^{-1}$)

But $a = a^{-1} \Rightarrow a^2 = 1 \iff a = 1$ or -1.

Thus $1, 2, \ldots, p-1$ consists of some pairs a, a^{-1}, and 1 and -1.

Multiply: $(p-1)! = 1^{p-3/2} \cdot 1 \cdot -1 = \underline{-1}$. □

Is -1 a square in $\mathbb{Z}_p$?

e.g. in $\mathbb{Z}_5$: $x = 2$ has $x^2 = -1$ ✓

$\mathbb{Z}_7$: $0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 2$ ✗

(don't need to check $4, 5, 6$ as $-x$ squares to x^2)

$\mathbb{Z}_{13}$: $x = 5$: $5^2 = -1$

$\mathbb{Z}_{19}$: ✗ (can check)

Proposition 13 Let p be an odd prime. Then -1 is a square number mod p iff $p \equiv 1 \pmod 4$.

Proof First consider $p = 4k+3$ ($k \in \mathbb{N}_0$). Suppose for contradiction that $x^2 = -1$ (in $\mathbb{Z}_p$)

We have $x^{4k+2} = 1$ (FLT)

But $x^{4k+2} = (x^2)^{2k+1} = (-1)^{2k+1} = -1$ ⁂

For $p = 4k+1$, have $(4k)! = -1$ (Wilson)

Compare $(4k)! = 1 \times 2 \times \ldots \times 2k\,(2k+1)(2k+2)\ldots(4k)$

with $(2k)!^2 = 1 \times 2 \times \ldots \times 2k \times 1 \times 2 \times \ldots \times 2k$

We have $4k = -1,\ 4k-1 = -2,\ \ldots,\ 2k+1 = -2k$

So $(2k)!^2 = (4k)!\,(-1)^{2k} = (4k)! = -1$. ✓

□

Solving Congruence Equations

1) Solve $7x \equiv 4 \bmod 30$

Finding a solution: Have $(7, 30) = 1$ so can run Euclid on 7 and 30 to find $13 \times 7 - 3 \times 30 = 1$

so $13 \times 7 \equiv 1 \bmod 30$

so $52 \times 7 \equiv 4 \bmod 30$

So $x = 52$ is a solution.

Other solutions: $x' \equiv 52 \bmod 30$ also works

No more solutions: If x' is a solution, want to show $x' \equiv 52 \bmod 30$.

Have $7x \equiv 4 \bmod 30$, $7x' \equiv 4 \bmod 30$

so $7x \equiv 7x' \bmod 30 \Rightarrow x \equiv x' \bmod 30$

as 7 is invertible. □

Shorter method: $7x \equiv 4 \bmod 30$

$\Leftrightarrow$ $13 \times 7x \equiv 13 \times 4 \bmod 30$ (13 invertible)

(13 ↑ inverse)

$\Leftrightarrow$ $x \equiv 52 \bmod 30$

This is faster if you spot the inverse.

2) Solve $10x \equiv 12 \bmod 34$.

$10x \equiv 12 \pmod{34} \Leftrightarrow 10x = 12 + 34y, \ y \in \mathbb{Z}$

$\Leftrightarrow$ ~~$5x \equiv$~~ $5x = 6 + 17y$

$\Leftrightarrow 5x \equiv 6 \bmod 17$

and then solve as before.

A simultaneous congruence?

Do we expect a solution to $x \equiv 6 \bmod 17$

$x \equiv 2 \bmod 19$

We guess yes, as 17 and 19 are coprime so "mod 17" and "mod 19" should be independent.

How about: $x \equiv 6 \bmod 34 \rightarrow x$ even

$x \equiv 11 \bmod 36 \rightarrow x$ odd ✗

34 and 36 aren't coprime.

Theorem 14 (Chinese Remainder theorem) Let u, v be coprime.

Then for any a, b, there is an x with $x \equiv a(u)$, $x \equiv b(v)$.
Moreover the solution is unique mod uv.

Proof Existence: Have $su + tv = 1$ for some $s, t \in \mathbb{Z}$ (as u, v coprime).

Now, $su \equiv 0(u)$, $su \equiv 1(v)$

$tv \equiv 1(u)$, $tv \equiv 0(v)$

Hence $x = a(tv) + b(su)$ has $x \equiv a(u), b(v)$ ✓

Uniqueness: Certainly any $x' \equiv x(uv)$ is also a solution.

Now suppose $x' \equiv a(u)$, $x' \equiv b(v)$.

so $x' \equiv x(u)$, $x' \equiv x(v)$

$\Rightarrow u \mid x' - x$, $v \mid x' - x$

but u, v are coprime, so $uv \mid x' - x$

So $x' \equiv x(uv)$. ✓ □

Remark Similarly, if $u_1, u_2, \ldots, u_k$ are pairwise coprime then $\forall a_1, \ldots a_k \ \exists x$ such that $x \equiv a_1(u_1)$, $\ldots$ $x \equiv a_i(u_i)$, $\ldots$, $x \equiv a_k(u_k)$ by induction.

An application of Fermat-Euler (RSA coding)

Normally to send a coded message

Pick 2 large distinct primes p, q. Let $n = pq$.

Fix a "coding exponent" e. To encode a message $x \in \mathbb{Z}_n$, raise to power e in $\mathbb{Z}_n$. $x \to x^e \mod n$

take $hcf(x, n) = 1$ usually fine if $x \ll n$

How to decode? Seek d such that $x^{ed} = x$.

We know $x^{\phi(n)} = 1$ in $\mathbb{Z}_n$

so $x^{k\phi(n)} = 1 \quad \forall k \in \mathbb{Z}$

$x^{k\phi(n)+1} = x$

We want d with ed of form $k\phi(n) + 1$ (some $k \in \mathbb{Z}$)

i.e. $ed \equiv 1 \mod \phi(n)$

Easy to solve by running Euclid on e and $\phi(n)$ assuming $hcf(e, \phi(n)) = 1$.

To encode: $x \to x^e$ in $\mathbb{Z}_n$, so need to know n, e

To decode: $y \to y^d$ in $\mathbb{Z}_n$, so need n, d i.e. need $n, e, \phi(n)$

$\phi(n) = n - p - q + 1$

So need to know how to factorise n (hard)

This is the end of Chapter 1 (elementary NT)

Chapter 2: The Reals

The Need for the Reals

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

Proposition 1 There is no rational x with $x^2 = 2$.
(may assume $x > 0$, as $(-x)^2 = x^2$)

Proof 1 Suppose $x^2 = 2$ for $x = \frac{a}{b}$, $a, b \in \mathbb{N}$

So $\frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2$

but exponent of 2 in prime factorisation a^2 is even and in b^2 it's odd, contradicting unique factorisation. □

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

Proof 2 Suppose $x^2 = 2$, $x = \frac{a}{b}$ where $a, b \in \mathbb{N}$

So for any $c, d \in \mathbb{Z}$: $cx + d$ is of the form $\frac{e}{b}$ for some $e \in \mathbb{Z}$.

And so $cx + d > 0 \Rightarrow cx + d \geq \frac{1}{b}$

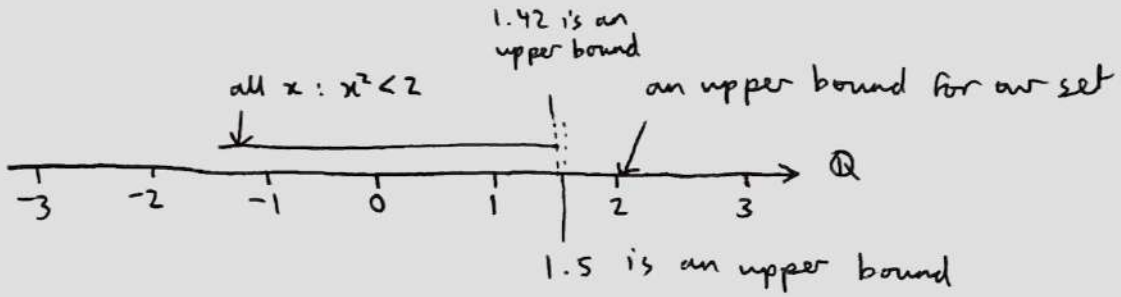
But $0 < x - 1 < 1$ (as $1 < x < 2$, ↑ from $x^2 = 2$)

So $0 < (x-1)^n < \frac{1}{b}$ for sufficiently large n

This is a contradiction because $(x-1)^n$ is of the form $cx + d$ where $c, d \in \mathbb{Z}$ (using $x^2 = 2$). # □

So "$\mathbb{Q}$ has a gap"

How to express this mentioning only $\mathbb{Q}$?



In $\mathbb{Q}$ there is no least upper bound (working in $\mathbb{Q}$: "$\sqrt{2}$" does not exist)

↑ This is how we say inside $\mathbb{Q}$ that "$\mathbb{Q}$ has a gap"

What we assume about the reals:

The reals are a set written $\mathbb{R}$ with elements 0 and 1 ($0 \neq 1$) equipped with operations $+$ and $\times$ and an ordering "$<$" such that

1. $+$ is commutative and associative (identity 0), every x has inverse
2. $\times$ is commutative and associative (identity 1) and every nonzero x has an inverse
3. $\times$ is distributive over $+$: $a(b+c) = (ab)+(ac)$
4. $\forall a, b$, exactly one of $a<b$, $a=b$, $a>b$ holds and $a<b,\ b<c \Rightarrow a<c$
5. $\forall a, b, c$: $a<b \Rightarrow a+c<b+c$
   $c>0$: $a<b \Rightarrow ac<bc$
6. For any set S of reals that is non-empty and bounded above, S has a least upper bound. (Least upper bound axiom)

PTO

S is bounded above if $\exists x \in \mathbb{R}$ with $x \geq y \ \forall y \in S$.

Such an x is an <u>upper bound</u> for S.

Say x is the least upper bound of S if x is an upper bound for S and every other upper bound of S is at least x.

Numbers and Sets - Lecture 10

29/10/20

Remarks

1. From rules 1-5, can check e.g. $0 < 1$
   If not then $1 < 0 \Rightarrow 0 < -1$
   so $0 < 1$ (multiplying by "positive" -1) $*$
2. May view $\mathbb{Q}$ as contained in $\mathbb{R}$ by identifying $\frac{a}{b} \in \mathbb{Q}$ with $ab^{-1} \in \mathbb{R}$
3. Least upper bound axiom (6) is false in $\mathbb{Q}$.
4. Why "non-empty and bounded above" in (6)?
   - If S is not bounded above then it has no upper bound so no least one
   - If S is empty then every $x \in \mathbb{R}$ is an upper bound so no least one.
5. Can construct $\mathbb{R}$ from $\mathbb{Q}$ and check axioms.

Examples of sets and least upper bounds

1. $S = \{ x \in \mathbb{R} : 0 \leq x \leq 1 \}$ $\quad [0, 1]$ $\quad$ L.U.B of S is $\sup(S)$

$x \leq 2 \quad \forall x \in S$ $\quad$ ~~$x \leq \frac{3}{4} \quad \forall x \in S$~~ $\quad$ but "$x \leq \frac{3}{4}$" is not an upper bound.

Least upper bound for S is 1.

1 is an upper bound: $x \leq 1 \quad \forall x \in S$

Every upper bound y must have $y \geq 1$ as $1 \in S$.

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

$\sup S = 1$ because 1 is an upper bound $(x \leq 1 \quad \forall x \in S)$.

~~No upper bound $c < 1$ as $1 + \frac{c}{2} \in S$~~

No upper bound $c < 1$: $\left(c \geq \frac{1}{2} \text{ as } \frac{1}{2} \in S \right)$

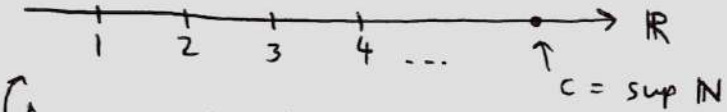
If $c \leq 1$ then $0 < c < 1$ so $\frac{1+c}{2} \in S$, $\frac{1+c}{2} > c$. $\#$

3. $S = \{ 1 - \frac{1}{n} : n \in \mathbb{N} \}$

1 is an upper bound. Is there an upper bound less than 1?

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

Proof



Assume not. Then $\exists\, c \in \mathbb{R} : c = \sup \mathbb{N}$.

So $c-1$ is not an upper bound for n (c is L.U.B).

So $\exists\, n \in \mathbb{N} : n > c-1$.

But then $n+1 \in \mathbb{N}$, $n+1 > c$ ⚡ □

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

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

So $\frac{1}{n} < t$. □

Note that these results show that $\mathbb{R}$ doesn't contain "infinitely big" or "infinitesimally small" elements.

Back to example 3: do have $\sup S = 1$ because suppose $c < 1$ is an upper bound. Then $1 - \frac{1}{n} < c \quad \forall n \in \mathbb{N} \Rightarrow 1 - c < \frac{1}{n} \quad \forall n$ but $1 - c > 0$ whilst $\frac{1}{n}$ can be made arbitrarily small (see Corollary 3) so impossible. □

Warning: If S has a greatest element (like $[0,1]$) then that greatest element is $\sup S$. So $\sup S \in S$.
But if S has no greatest element e.g. $(0,1)$ then $\sup S \notin S$.

Note If S is a nonempty set of reals that is bounded below ($\exists x$ s.t. $x \leq y \ \forall y \in S$)
Then the set $-S = \{-y : y \in S\}$ is non-empty and bounded above, so has a least upper bound c.
So $-c$ is the greatest lower bound of S - the infimum of S or $\inf S$.

In particular, if S is non-empty and bounded above and below, then it has a sup. and inf.

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

Proof Let $S = \{x \in \mathbb{R} : x^2 < 2\}$
Have S nonempty (e.g. $1 \in S$) and bounded above (e.g. 2 is an upper bound)
So S has a sup, C such that $1 \leq c \leq 2$.

Claim $c^2 = 2$

Proof of claim Suppose not. If $c^2 < 2$

For $0 < t < 1$, have $(c+t)^2 = c^2 + 2ct + t^2 \leq c^2 + 5t$
as $2ct \leq 2c$, $t^2 < t$

and $c^2 + 5t < 2$ for $t < \frac{2-c^2}{5}$

so contradicts c being an upper bound for S.

If $c^2 > 2$: have $0 < t < 1$, $(c-t)^2 = c^2 - 2ct + t^2$

$\geq c^2 - 4t > 2$ for t small $\left(t < \frac{c^2-2}{4}\right)$

contradicting c being least upper bound:

$c - t < c$ also an upper bound $\lightning$

So $c^2 = 2$.

Remark Same proof shows that $\sqrt[n]{x}$ exists $\forall n \in \mathbb{N}$, $x \in \mathbb{R}$, $x > 0$.

A real that is not rational is called irrational

e.g. $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$, $\sqrt{15}$.

Claim $2 + 3\sqrt{5}$ is irrational

Proof If $2 + 3\sqrt{5} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$

Then $\sqrt{5} = \frac{a-2b}{3b} \in \mathbb{Q}$. $\lightning$

Also "the rationals are dense": if $a, b \in \mathbb{R}$, $a < b$

then $\exists\, c \in \mathbb{Q}$: $a < c < b$.

May assume $a, b \geq 0$

Choose $n \in \mathbb{N}$ with $\frac{1}{n} < b - a$

Among $\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots$ there is a final one that is $\leq a$, say

$\frac{q}{n}$ (else a would be an upper bound for $\left\{\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots\right\}$

contradicting axiom of Archimedes)

So $a < \frac{q+1}{n} < b$ ✓

Also "the irrationals are dense": $\forall a, b \in \mathbb{R}$, $a < b$,
$\exists$ irrational c with $a \leq c < b$.

Indeed $\exists$ rational c with $a\sqrt{2} < c < b\sqrt{2}$, so

$a < \frac{c}{\sqrt{2}} < b$. ✓

What should "$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$" mean?

How about "$0.33333\ldots = \frac{1}{3}$"?

Presumably, that $1,\ 1+\frac{1}{2},\ 1+\frac{1}{2}+\frac{1}{4}, \ldots$ should "tend to" 2

$0.3,\ 0.33,\ 0.333, \ldots$ should "tend to" $\frac{1}{3}$

This <u>isn't</u> the same as "x_n are getting closer and closer to c"

It's <u>not</u> "$\forall \varepsilon > 0$ $\exists n$ with $c - \varepsilon < x_n < c + \varepsilon$"

We want the sequence to get and <u>stay</u> within ε of c.

We say that $x_1, x_2, x_3, \ldots$ <u>tends to</u> c if

$\forall \varepsilon > 0$ $\exists N$ s.t. $\forall n \geq N$ have $c - \varepsilon < x_n < c + \varepsilon$.

$(|x_n - c| < \varepsilon)$

In $\mathbb{R}$ $|a|$ of $a \in \mathbb{R}$ is a if $a \geq 0$

$-a$ if $a < 0$

If x_n tends to c, can write $x_n \to c$ (as $n \to \infty$)

Examples

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

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

Claim $x_n \to 1$

Proof Given $\varepsilon > 0$

Choose $N \in \mathbb{N}$ with $N > \frac{1}{\varepsilon}$ (or $\frac{1}{N} < \varepsilon$)

Then $\forall n \geq N$: $|x_n - 1| = \frac{1}{2^n} \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$

✓ □

2. The constant sequence $c, c, c, c, \ldots$ $(x_n = c \ \forall n)$

Claim $x_n \to c$

Proof Given $\varepsilon > 0$:

Have $|x_n - c| < \varepsilon \ \forall n$

□

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

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

Proof Suppose $x_n \to c$. Choose $\varepsilon = 1$:

So $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$ have $|x_n - c| < 1$.

$|1 - c|$ and $|(-1) - c| < 1$

So by Δ inequality $|1 - (-1)| < 2$ which is a contradiction.

□

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

$1, 0, \frac{1}{3}, 0, \frac{1}{5}, 0, \frac{1}{7}, \ldots$

PTO

Claim $x_n \to 0$

Proof Given $\varepsilon > 0$:

Choose $N \in \mathbb{N}$ with $\frac{1}{N} < \varepsilon$

Then $\forall n \geq N$: $x_n = \frac{1}{n}$ or 0, so $|x_n - 0| \leq \frac{1}{n} \leq \frac{1}{N} < \varepsilon$

□

Notes - If $x_n \to c$ for some c, then $x_1, x_2, x_3, \ldots$ is convergent. or (x_n) or $(x_n)_{n=1}^{\infty}$

Otherwise, it is divergent.

- Same idea as example 3: shows limits are unique.

Suppose $x_n \to c$, $x_n \to d$.

Suppose $c \neq d$ and choose $\varepsilon = \frac{1}{2}|c-d|$

Then $\exists N \in \mathbb{N}$ with $|x_n - c| < \varepsilon \quad \forall n \geq N$

and $\exists M \in \mathbb{N}$ with $|x_n - d| < \varepsilon \quad \forall n \geq M$

Now for any $n \geq \max(M, N)$, have

$|x_n - c|, |x_n - d| < \varepsilon$ so $|c-d| < 2\varepsilon$ ✱ as $|c-d| = 2\varepsilon$.

□

- Given a series $\sum_{n=1}^{\infty} x_n$, $\sum_{n=1}^{k} x_n$ is the "k^{th} partial sum"

Limits do behave as we expect.

e.g. If $x_n \leq d \ \forall n$ and $x_n \to c$, then $c \leq d$.

Suppose $c > d$. Choose $\varepsilon = |c-d|$, then

$\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$ have $|x_n - c| < \varepsilon$

but $|x_n - c| < \varepsilon \Rightarrow x_n > d$ ✱

□

Warning If $x_n < d$ and $x_n \to c$, need not have $c < d$:

e.g. $\frac{1}{2}, \frac{1}{2}+\frac{1}{4}, \frac{1}{2}+\frac{1}{4}+\frac{1}{8}, \ldots \to 1$

and all $x_n < 1$ so here "$c = d$".

How about $x_n + y_n$?

Proposition 5 If $x_n \to c$ and $y_n \to d$, then $x_n + y_n \to c + d$.

Idea: "late x_n are close to c, late y_n are close to d"

Proof Given $\varepsilon > 0$:

Have $x_n \to c$ so $\exists N \in \mathbb{N}$ s.t. $|x_n - c| < \frac{\varepsilon}{2}$ $\forall n \geq N$.

Also $y_n \to d$ so $\exists M \in \mathbb{N}$ s.t. $|x_n - d| < \frac{\varepsilon}{2}$ $\forall n \geq M$.

$\therefore$ for all $n \geq \max(M, N)$ have

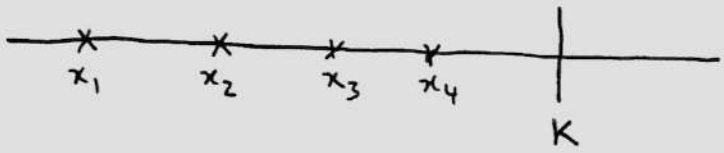
$$|(x_n + y_n) - (c+d)| \leq |x_n - c| + |y_n - d| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

$\uparrow$ Δ ineq. $\square$

Remark If we'd used "$|x_n - c| < \varepsilon$" instead of "$|x_n - c| < \frac{\varepsilon}{2}$", then at the end would have got $|(x_n + y_n) - (c+d)| < 2\varepsilon$ instead which is still fine, as ε could be replaced with $\frac{\varepsilon}{2}$.

A sequence $x_1, x_2, \ldots$ is <u>increasing</u> if $x_{n+1} \geq x_n \quad \forall n$.

Theorem 6 If $x_1, x_2, \ldots$ is increasing and bounded above, then it converges.



Remark If we lived in $\mathbb{Q}$ then this would be false:

e.g. 1, 1.4, 1.41, 1.414, 1.4142 "$\to \sqrt{2}$"

but $\sqrt{2} \notin \mathbb{Q}$.

Proof Let $c = \sup(x_1, x_2, \ldots)$

Claim $x_n \to c$

Proof Given $\varepsilon > 0$:

$\exists n$ s.t. $x_n > c - \varepsilon$ (else $c - \varepsilon$ is an upper bound $< c$)

So $\forall n \geq N$:

$c - \varepsilon < x_N \leq x_n < c$

so $\underline{|x_N - c| < \varepsilon}$ □

So "a bounded monotone sequence is convergent"

↑ increasing or decreasing

1) **Proposition 7** i) $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges

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

Note: there is no closed form for $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$

or $1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2}$

Idea $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \dots$

$$\geq 1 + \underbrace{\frac{1}{2}}_{\frac{1}{2}} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{\frac{1}{2}} + \frac{1}{16} + \dots$$

Proof (i) Have $\frac{1}{3} + \frac{1}{4} \geq \frac{1}{2}$

$$\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \geq \frac{1}{2}$$

In general $\frac{1}{2^n+1} + \frac{1}{2^n+2} + \dots + \frac{1}{2^{n+1}} \geq \frac{2^n}{2^{n+1}} = \frac{1}{2}$ $\forall n$

Hence partial sums of $\sum_{n=1}^{\infty} \frac{1}{n}$ are unbounded.

So it is not convergent.

(ii) **Idea** $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{8^2} + \dots$

$$\leq 1 + \underbrace{\frac{1}{2^2} + \frac{1}{2^2}}_{\frac{2}{2^2}} + \underbrace{\frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2}}_{\frac{4}{4^2}} + \underbrace{\frac{1}{8^2} + \dots}_{\frac{8}{8^2}}$$

$$= 1 + \frac{1}{2} + \frac{1}{4} + \dots$$

We have $\frac{1}{2^2} + \frac{1}{2^2} \leq \frac{2}{2^2} = \frac{1}{2}$ $\quad \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} \leq \frac{4}{4^2} = \frac{1}{4}$

In general $\frac{1}{(2^n)^2} + \frac{1}{(2^n+1)^2} + \dots + \frac{1}{(2^{n+1}-1)^2} \leq \frac{2^n}{(2^n)^2} = \frac{1}{2^n}$

So partial sums are bounded. (by $1 + \frac{1}{2} + \frac{1}{4} + \dots = 2$) $\forall n$.

□

Remarks

1) $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ is called the harmonic series

2) $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ - proved in Part II Linear Analysis

3) Decimal Expansions - what should "$0.a_1 a_2 a_3 \ldots$" mean?

It should be the limit (if it exists) of

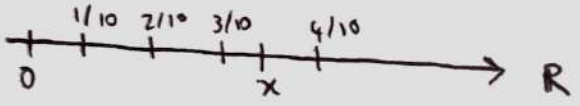
$0.a_1,\ 0.a_1 a_2,\ 0.a_1 a_2 a_3,\ \ldots$

So define $0.a_1 a_2 a_3 \ldots = \sum_{n=1}^{\infty} \frac{a_n}{10^n}$

(converges as all terms > 0 and partial sums bounded e.g. by 1)

Conversely given $x \in \mathbb{R}$, $0 < x < 1$, want to write

$x = 0.a_1 a_2 a_3 \ldots$ for some $a_1, a_2, \ldots \in \{0, 1, \ldots, 9\}$



Choose the greatest a_1 in $\{0, 1, \ldots, 9\}$ with $\frac{a_1}{10} \leq x$

So $0 \leq x - \frac{a_1}{10} < \frac{1}{10}$.

Now greatest $a_2 \in \{0, 1, \ldots, 9\}$ s.t. $\frac{a_1}{10} + \frac{a_2}{100} \leq x$

So $0 \leq x - \frac{a_1}{10} - \frac{a_2}{100} < \frac{1}{100}$.

Inductively: we obtain $a_1, a_2, a_3, \ldots \in \{0, 1, \ldots, 9\}$

such that $0 \leq x - \sum_{n=1}^{k} \frac{a_n}{10^n} < \frac{1}{10^k} \quad \forall\, k$

Thus $\sum_{n=1}^{\infty} \frac{a_n}{10^n} = x$, i.e. $0.a_1 a_2 a_3 \ldots = x$.

Remarks

1. A decimal expansion $0.a_1 a_2 a_3 \ldots$ is <u>recurrent</u> if $a_{n+k} = a_n \quad \forall n \geq N$, some N and k.

   e.g. $0.3178426426426426\ldots$

   Can check $x = 0.a_1 a_2 \ldots$ is recurrent iff x is rational.

2. Decimal expansions need not be unique:

   $0.3700000\ldots = 0.3699999\ldots$

3. That's the only way to have non-unique expansions

   If $0.a_1 a_2 \ldots$, $0.b_1 b_2 \ldots$, are the ~~sss~~ decimal expansions (different) of the same number then $\exists N \in \mathbb{N}$ where

   $a_n = b_n \quad \forall n < N$

   $a_N = b_N - 1$, $\quad a_n = 9, b_n = 0 \quad \forall n > N$

   or vice versa.

The number e

Define $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots$

$\uparrow \quad \uparrow \quad \uparrow \quad \uparrow$

$1 \quad 1 \quad \geq \frac{1}{2} \quad \geq \frac{1}{4}$

Partial sums are bounded by $1 + 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 3$, and all terms are > 0. ($\frac{1}{n!} < \frac{1}{2^{n-1}}$ $\forall n \geq 2$, inductively)

If we write $0! = 1$ then $e = \sum_{n=0}^{\infty} \frac{1}{n!}$

Say $x \in \mathbb{R}$ is algebraic if it is a root of a non-zero polynomial with integer coefficients.

i.e. $a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0 = 0$

where $a_i \in \mathbb{Z}$, for some $d \in \mathbb{Z}$ $(a_d \neq 0)$.

Every rational is algebraic : $\frac{p}{q}$ is a root of $qx - p = 0$

$\sqrt{2}$ is algebraic : $x^2 - 2 = 0$

$\sqrt{2} + 1$ is algebraic : $((\sqrt{2} + 1) - 1)^2 = 2$ so $(x-1)^2 - 2 = 0$.

Are all reals algebraic?

Proposition 8 e is irrational.

Proof Suppose rational : $e = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q > 1$

$\Rightarrow q! e = $ (some integer)

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

So $\underbrace{q! + \frac{q!}{1!} + \frac{q!}{2!} + \dots + \frac{q!}{q!}}_{\text{an integer}} + \frac{q}{(q+1)!} + \frac{q}{(q+2)!} + \dots$

Also $\frac{q!}{(q+1)!} = \frac{1}{q+1}$, $\frac{q!}{(q+2)!} = \frac{1}{(q+1)(q+2)} \leq \frac{1}{(q+1)^2}$

Generally $\frac{q!}{(q+n)!} \leq \frac{1}{(q+1)^n}$

so $\sum_{n=q+1}^{\infty} \frac{q!}{n!} \leq \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+2)^2} + \dots = \frac{1}{q} < 1$

as $q \geq 2$.

So this is not an integer, contradicting the assumption that $\sum_{n=0}^{\infty} \frac{q!}{n!}$ is an integer. ※ □

A real that is not algebraic is called <u>transcendental</u>.

<u>Theorem 9</u> The number $c = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

$c = 0.110001000000000000000000010000\dots$

To prove, we need 2 facts about polynomials.

<u>Fact 1</u> For any polynomial P, $\exists$ a constant k such that

$$|P(x) - P(y)| \leq k|x-y| \qquad \forall\ 0 \leq x, y \leq 1$$

<u>Proof</u> $P(x) = a_d x^d + \dots + a_0$

$P(x) - P(y) = a_d(x^d - y^d) + a_{d-1}(x^{d-1} - y^{d-1}) + \dots + a_1(x-y)$

$= (x-y)\left[a_d(x^{d-1} + x^{d-2}y + \dots + y^{d-1}) + \dots + a_1\right]$

So $|P(x) - P(y)| \leq |x-y|\left[(|a_d| + |a_{d-1}| + \dots + |a_1|)\,d\right]$ as $0 \leq x, y \leq 1$.

□

Fact 2 A nonzero polynomial of degree d has $\leq d$ roots.

Proof Given a polynomial p of degree d:

If p has no roots it's certainly true

If p has a root, have $\underline{a}$ a root:

$p(x) = (x-a)\,q(x)$ for some q of degree $d-1$.

So each root of p is either a or a root of q but q has at most $d-1$ roots inductively. □

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

Suppose for contradiction that polynomial P has c as a root.

Then $\exists k$ with $\left|\frac{P(x)-P(y)}{x-y}\right| \leq k|x-y| \quad \forall\, 0 \leq x, y \leq 1$

Say P has degree d: $P(x) = a_d x^d + \dots + a_0$ ($a_i \in \mathbb{Z}$, $a_d \neq 0$)

Now $|c - c_n| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \leq \frac{2}{10^{(n+1)!}}$

Also $c_n = \frac{a}{10^{n!}}$ for some $a \in \mathbb{Z}$ so $P(c_n) = \frac{b}{10^{d\,n!}}$ ($b \in \mathbb{Z}$)

(since $P\left(\frac{s}{t}\right) = \frac{q}{t^d}$ for some $q \in \mathbb{Z}$ whenever $s, t \in \mathbb{Z}$)

But for n large enough, c_n is not a root of p as finitely many roots. So $|P(c_n)| \geq \frac{1}{10^{d\,n!}}$ i.e. $|P(c_n) - P(c)| \geq \frac{1}{10^{d\,n!}}$

Thus $\frac{1}{10^{d\cdot n!}} \leq k\,\frac{2}{10^{(n+1)!}}$, a contradiction for n sufficiently large. □

(I may write this up better)

Written up in LaTeX – see Overleaf doc

Remarks 1. Same proof shows that any real x such that

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

is transcendental.

"x has very good rational approximations"

2. Such x are called <u>Liouville numbers</u> so could view Thm 9 as "every Liouville number is transcendental"

3. Theorem 9 does not show e is transcendental (but it is).

4. Another proof of existence of transcendentals is in Ch 4.

Numbers and Sets - Lecture 15

10/11/20

The Complex Numbers

Some polynomials have no real roots e.g. $x^2 + 1 = 0$

We'll try to "force" an x with $x^2 = -1$

The complex numbers $\mathbb{C}$ consist of $\mathbb{R}^2$ with operations $+$ and $\times$, defined by $(a,b) + (c,d) = (a+c, b+d)$

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

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

Let $i = (0,1)$ then $i^2 = (0,1) \cdot (0,1) = (-1,0) = \underline{-1}$

Note that every $z \in \mathbb{C}$ is of the form $a + bi$, $a, b \in \mathbb{R}$

Remarks

1. $\mathbb{C}$ obeys all usual algebraic rules (note $\mathbb{C}$ is a field)
2. Every nonzero polynomial (even with complex coefficients) has a root in $\mathbb{C}$.
   This is the Fundamental Theorem of Algebra

Chapter 3 - Sets and Functions

Definition A set is a collection of mathematical objects

e.g. $\mathbb{R}$, $\mathbb{N}$, $\{1, 5, 9\}$, $[0, 1]$

Two sets with the same members are the same.

If $\forall x$, $x \in A \iff x \in B$ then $A = B$.

(Note $\{3, 4, 4, 6\} = \{3, 4, 6\}$)

Subsets Given set A and property $P(x)$, can form $\{x \in A : P(x)\}$, the subset of A with property P.

B is a subset of A if $\forall x$: $x \in B \Rightarrow x \in A$.

Written $B \subset A$ or $B \subseteq A$.

We have $A = B \iff A \subseteq B,\ B \subseteq A$

Unions and Intersections

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

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

A and B are **disjoint** if $A \cap B = \emptyset$ ← empty set

Intersection is a special case of subset selection

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

Difference: $A \setminus B = \{x \in A : x \notin B\}$

$\cup$ is distributive over $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

and $\cap$ over $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (*)

Prove (*):

LHS $\subset$ RHS: Given $x \in A \cap (B \cup C)$

$\Rightarrow$ $x \in A$ and either $x \in B$ or $x \in C$

If $x \in B$ have $x \in A$, $x \in B$

So $x \in A \cap B \Rightarrow x \in$ RHS

Same for $x \in C$ case.

RHS $\subset$ LHS: Given $x \in (A \cap B) \cup (A \cap C)$

WLOG if $x \in (A \cap B)$ then $x \in A$ and $x \in B \cup C$

so $x \in$ LHS.

□

Can have bigger unions e.g. infinite union $\bigcup_{n=1}^{\infty} A_n = \bigcup_{n \in \mathbb{N}} A_n$ ← index set

Not defined as a limit

Numbers and Sets - Lecture 16

11/11/20

Ordered Pairs

For any a, b can form ordered pair (a, b)

$(a, b) = (c, d) \iff a = c$ and $b = d$

For sets A and B, can form their product $A \times B$, the set of all ordered pairs $\{(a, b) : a \in A, b \in B\}$.

e.g. can view $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ as a plane.

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

Power Sets

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

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

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

Note / Warning For a set A, can form $\{x \in A : p(x)\}$ but cannot form $\{x : p(x)\}$

If we could, then consider $\{x : x \notin x\} = X$

Does $X \in X$? If yes: then $X \notin X$ by defn of X

If no: $X \notin X$ so $X \in X$ by defn of X ⁂

(Russell's paradox)

Similarly, there is no "universal set" Y with $x \in Y$ $\forall x$. Otherwise could form X above by subset selection.

To guarantee a given set exists, must somehow obtain it from known sets.

Finite Sets

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

For $n \in \mathbb{N}_0$, say set A has <u>size n</u> if we can write $A = \{a_1, a_2, \dots, a_n\}$ with a_i distinct.

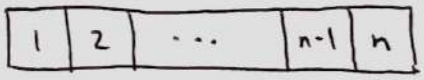
Say A is finite if $\exists\, n \in \mathbb{N}_0$ where A has size n (otherwise infinite)

Note A cannot have size m <u>and</u> size n for $n \neq m$.
Suppose A has size m and size n, $n, m > 0$.
Then, removing an element, we get a set of size $n-1$ and $m-1$ – done by induction (on max element).

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

Proof 1 May assume set is $\{1, 2, \dots, n\}$ WLOG.
To specify a subset S we must say if $1 \in S$ or $1 \notin S$, then if $2 \in S$ or $2 \notin S$, and so on.
So no. of choices is $\underbrace{2 \times 2 \times \dots \times 2}_{n \text{ times}} = \underline{2^n}$. □

Proof 2 Induction on n: $n = 0$ ✓
Take $n > 0$.



For $T \subseteq \{1, 2, \dots, n-1\}$, how many $S \subseteq \{1, \dots, n\}$ have $S \cap \{1, \dots, n-1\} = T$?
Exactly 2: T and $T \cup \{n\}$.
Hence # subsets of $\{1, 2, \dots, n-1\} \times 2$ is # subsets of $\{1, \dots, n\}$ so done by induction. □

If A has size n then <u>$|A| = n$</u>

Binomial Coefficients

For $n \in \mathbb{N}_0$ $0 \leq k \leq n$, write $\binom{n}{k}$ for number of subsets of an n-set that are of size k. (n-set: size n)

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

Note that $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, $\binom{n}{1} = n$ $(n > 0)$

Note also that $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$ because we are counting all subsets.

Also

1. $\binom{n}{k} = \binom{n}{n-k}$ $\quad n \in \mathbb{N}_0, \ 0 \leq k \leq n$

2. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

   # k-subsets of $\{1, \ldots, n\}$ without n is $\binom{n-1}{k}$

   # k-subsets of $\{1, \ldots, n\}$ is $\binom{n-1}{k-1}$ as we choose n and then pick remaining $k-1$ from $n-1$.

   So $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Pascal's Triangle

```
                1   1
            1   2   1
        1   3   3   1
    1   4   6   4   1
1   5   10  10  5   1
1   6   15  20  15  6   1
```

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

Proof # of ways to name an element is n, then $n-1$, ...

so # of ways to specify a k-set is

$n(n-1)(n-2)\dots(n-k+1)$

# of times a given k-set is named: $k!$

Hence # k-sets is $\dfrac{n(n-1)\dots(n-k+1)}{k!}$ □

Can also write $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

Notice $\binom{n}{3} \approx \dfrac{n^3}{6}$ for large n.

An application of binomial coefficients:

Theorem 3 (Binomial Theorem) $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \dots + \binom{n}{n}b^n$

$\forall a, b \in \mathbb{R},\ n \in \mathbb{N}$

Proof When we expand $(a+b)^n = (a+b)(a+b)\dots(a+b)$

we get terms of the form $a^k b^{n-k}$ $(0 \le k \le n)$

terms $a^k b^{n-k}$ is $\binom{n}{k}$ so have

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

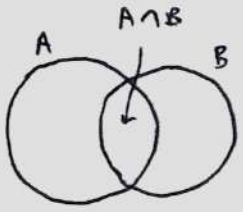
$$= \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k}$$ □

e.g. $(1+x)^n = 1 + nx + \dfrac{n(n-1)}{2}x^2 + \binom{n}{3}x^3 + \dots + nx^{n-1} + x^n$

so for x small, $(1+x)^n \approx 1 + nx$

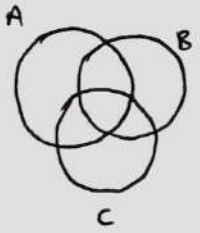
What can we say about the relationships between sizes of unions and intersections of finite sets?

e.g. $|A \cup B| = |A| + |B| - |A \cap B|$



to make sure $A \cap B$ not counted twice

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



Notation
$S_1 \cap S_2 = S_{\{1,2\}}$

Theorem 4 (Inclusion-Exclusion Theorem) Let $S_1, \dots, S_n$ be finite sets. Then $|S_1 \cup \dots \cup S_n|$ is

$$\sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \dots + (-1)^{n+1} \sum_{|A|=n} |S_A|$$

with S_A meaning $\bigcap_{i \in A} S_n$ and $\sum_{|A|=R | A \subseteq \{1,\dots,n\} \text{ of size } R}$ as a sum over all

Proof Let $x \in$ LHS : Say x belongs to S_i for k of the S_i.
We want x counted exactly once on RHS.

$\#\, A,\ |A| = 1$ with $x \in S_A = k$

$\#\, A,\ |A| = 2$ with $x \in S_A = \binom{k}{2}$ ← (must choose 2 of the i that it belongs to)

In general $\#\, A,\ |A| = r$ with $x \in S_A$ is $\binom{k}{r}$.

times x counted on RHS is

$$k - \binom{k}{2} + \binom{k}{3} - \dots + (-1)^{k+1}\binom{k}{k} = 1 - (1 + (-1))^k \quad \text{(by BT)}$$

$$= 1.$$

□

Functions

For sets A and B, a function from A to B is a rule that assigns each $x \in A$ a unique point $f(x) \in B$.

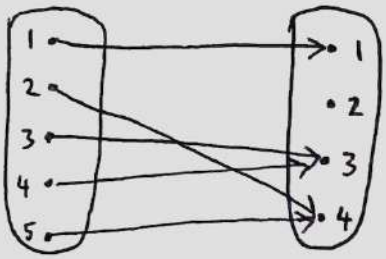
More precisely, a function from A to B is a set $f \subseteq A \times B$ with $\forall x \in A$ a unique $y \in B$ with $(x, y) \in f$.

If $(x, y) \in f$ then have $f(x) = y$.

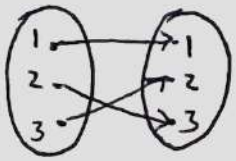
Examples
- $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$: can say "$f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$" or "$f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$"
- Not a function from $\mathbb{R} \to \mathbb{R}$ with $f(x) = \frac{1}{x}$: not defined for $x = 0$
- Not a function $\mathbb{R} \to \mathbb{R}$: $f(x) = \pm\sqrt{|x|}$ as $f(2)$ can be $\sqrt{2}$ and $-\sqrt{2}$: not unique
- $f(x) = \begin{cases} 1 & \text{if } x \text{ rational} \\ 0 & \text{if not} \end{cases}$ $f : \mathbb{R} \to \mathbb{R}$ (this is a valid function)

Examples of functions - cont.

5) $A = \{1, 2, 3, 4, 5\}$ $B = \{1, 2, 3, 4\}$



6)



Say $f: A \to B$ is <u>injective</u> if $\forall a, a' \in A$, then

$a \neq a' \Rightarrow f(a) \neq f(a')$

or equivalently $f(a) = f(a') \Rightarrow a = a'$.

"different points stay different"

Say $f: A \to B$ is <u>surjective</u> if $\forall b \in B$, $\exists a \in A$ with $f(a) = b$. "everything in B is hit"

Say $f: A \to B$ is <u>bijective</u> if it's injective and surjective.

"everything hits, exactly once" or "f pairs up A and B"

For $f: A \to B$: A is the <u>domain</u>, B is the <u>range</u>

The <u>image</u> of f is $\{f(a) : a \in A\} = \{b \in B : f(a) = b, a \in A\}$

Image is "everything that is hit"

e.g. for $f: \mathbb{R} \to \mathbb{R}$ $x \mapsto x^2$, image of f is $\{y \in \mathbb{R}; y \geqslant 0\}$

⚠ <u>Must</u> specify domain and range.

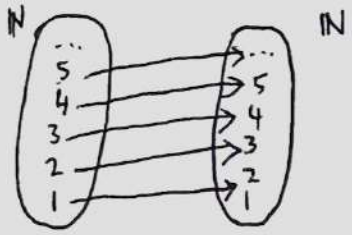
For A, B finite:

1. No surjection $A \to B$ if $|B| > |A|$
2. No injection $A \to B$ if $|A| > |B|$
3. For $f: A \to A$, f injective $\Leftrightarrow$ f surjective

4. No bijection $A \to B$ with $B \subseteq A$, $B \neq A$ (proper subset)

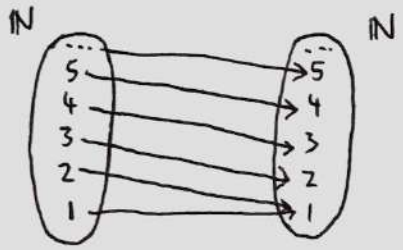
But for <u>infinite</u> sets:

1. Define $f_0 : \mathbb{N} \to \mathbb{N}$ by $x \mapsto x+1$



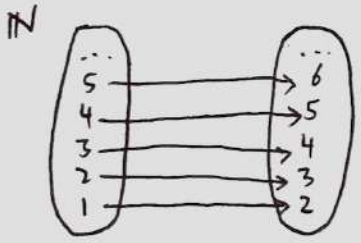
f_0 injective but not surjective

2. Define $f_1 : \mathbb{N} \to \mathbb{N}$ by $x \mapsto x-1$ if $x \neq 1$
$x \mapsto 1$ if $x = 1$



f_1 is surjective but not injective

3. Define $g : \mathbb{N} \to \mathbb{N} \setminus \{1\}$, $x \mapsto x+1$



G is a bijection from $\mathbb{N}$ to a proper subset of $\mathbb{N}$.

<u>More examples</u>

1. $1_X : X \to X$ with $x \mapsto x$, the identity function
2. For any set X with $A \subseteq X$, have <u>indicator / characteristic</u> function $\chi_A : X \to \{0, 1\}$

with $x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$

3. A sequence $x_1, x_2, \ldots$ of reals is a function $\mathbb{N} \to \mathbb{R}$: $n \mapsto x_n$
4. Operation $+$ on $\mathbb{N}$ is function $\mathbb{N}^2 \to \mathbb{N}$ with $(m, n) \mapsto m+n$

5. A set X has size n iff $\exists$ a bijection

$\{1, 2, \cdots, n\} \to X$ with $i \mapsto a_i$ $(X = \{a_1, a_2, \cdots, a_n\})$

Composition of Functions

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

e.g. $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x$ $\quad$ $g: \mathbb{R} \to \mathbb{R}$, $x \mapsto x+1$

$f \circ g(x) = 2(x+1)$

$g \circ f(x) = 2x + 1$

In general $\circ$ is not commutative.

Function composition is associative.

Given $f: A \to B$, $g: B \to C$, $h: C \to D$

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

Indeed for any $x \in A$:

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

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

The two compositions are equal $\forall x$ so are the same function. $\square$

Numbers and Sets – Lecture 19

19/11/20

Say $f: A \to B$ is invertible if $\exists\, g: B \to A$ with $gf = 1_A$ and $fg = 1_B$

e.g. $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x+1$ $\quad$ $g: \mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{x-1}{2}$

$(g \circ f)(x) = g(2x+1) = x$ so $g \circ f$ is $1_{\mathbb{R}}$

$(f \circ g)(x) = f\left(\frac{x-1}{2}\right) = x$ so $f \circ g$ is $1_{\mathbb{R}}$

So f is invertible: $g = f^{-1}$

In fact $f: A \to B$ is invertible iff it's a bijection.

$\Rightarrow$ If g is inverse to f: surjective: $\forall b \in B$, $b = f(g(b))$

injective: $\forall a, a' \in A$: $f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \Rightarrow a = a'$ ✓

$\Leftarrow$ Let $g(b)$ = the unique $a \in A$ with $f(a) = b$, for each $b \in B$. ✓

Equivalence Relations

A relation on a set X is a subset R of $X \times X$.

Usually write aRb for $(a,b) \in R$.

e.g. 1. on $\mathbb{N}$, aRb if $a \equiv b (5)$

2. on $\mathbb{N}$, aRb if $a \mid b$

3. on $\mathbb{N}$, aRb if $a \neq b$

4. on $\mathbb{N}$, aRb if $a = b \pm 1$

5. on $\mathbb{N}$, aRb if either $a, b \leq 6$ or $a, b > 6$

Some properties a relation might have:

1. R <u>reflexive</u> if $\forall x \in X$: xRx.

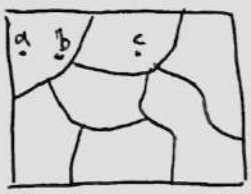
2. R <u>symmetric</u> if $\forall x, y \in X$: $xRy \Rightarrow yRx$

3. R <u>transitive</u> if $\forall x, y, z \in X$: $xRy, yRz \Rightarrow xRz$

Exercise: check examples – see which have what properties

An <u>equivalence relation</u> is reflexive, symmetric and transitive.

Example



Let X be a set, let $\{C_i : i \in I\}$ be a partition of X: each C_i nonempty, disjoint, $\bigcup_{i=I} C_i = X$

Then have $a R b$ if $\exists i$ s.t $a, b \in C_i$ is an equivalence relation.

All equivalence relations are of this form.

For an ER on X, $x \in X$, the equivalence class of x is

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

In Example 1 (xRy if $x \equiv y\ (5)$)

$\mathbb{N}$
$\equiv 0\ (5)$
$\equiv 1\ (5)$
$\equiv 2\ (5)$
$\equiv 3\ (5)$
$\equiv 4\ (5)$

Proposition 5 Let R be an equivalence relation on a set X. Then the equivalence classes partition X.

Proof Equivalence classes are all nonempty: xRx.

$$\bigcup_{x \in X} [X] = X \qquad (x \in [x] \ \forall x \in X)$$

↑ lowercase x

So need to show ECs are disjoint (or are the same).

Given x, y with $[x] \cap [y] \neq \emptyset$, need $[x] = [y]$.

Have $z \in [x] \cap [y]$, some z.

So zRx, $zRy \Rightarrow xRy$. $\forall t$, $tRx \Rightarrow tRy$ (transitivity)

$tRy \Rightarrow tRx$

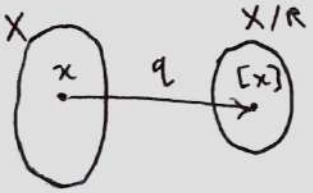
so $[x] = [y]$. □

Is there an equivalence relation on $\mathbb{N}$ with 3 ECs: 2 infinite, 1 finite?

Should think of this in terms of partitions then it becomes easy.

Given an ER on set X, the quotient of X by R is

$X/R = \{[x] : x \in X\}$ "the set of counties"



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

Another example: on $\mathbb{Z} \times \mathbb{N}$, define $(a,b)\ R\ (c,d)$ if $ad = bc$.

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

can think of as a copy of $\mathbb{Q}$ ~~$\mathbb{Z} \times \mathbb{N}$~~ $\mathbb{Z} \times \mathbb{N} / R$

Chapter 4 - Countability

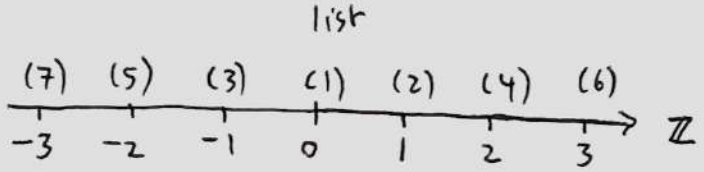
Looking at "sizes" of infinite sets e.g. $\mathbb{N}$ "looks smaller" than $\mathbb{Z}$

Say a set X is <u>countable</u> if X is <u>finite</u> or bijects with $\mathbb{N}$.

i.e. "you can list the elements" as $a_1, a_2, a_3, \ldots$ (may terminate).

<u>Examples</u>

1. Any finite set
2. $\mathbb{N}$
3. $\mathbb{Z}$



Can list as $0, 1, -1, 2, -2, 3, -3, \ldots, n, -n, \ldots$
so is countable

Write $a_n = \frac{n}{2}$ if n even, $-\frac{(n-1)}{2}$ if n odd

So in a sense "$\mathbb{Z}$ is the same size as $\mathbb{N}$"

Are <u>all</u> sets countable?

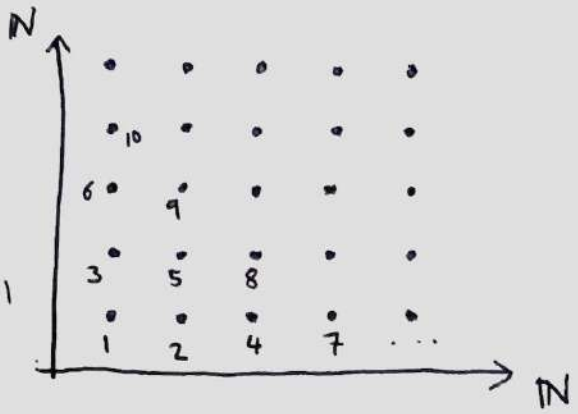
<u>Proposition 2</u> A set X is countable iff $\exists$ an injection $f: X \to \mathbb{N}$.

<u>Proof</u> If X finite then X injects into $\mathbb{N}$
If X bijects then it injects into $\mathbb{N}$. $\Rightarrow$ ✓

$\Leftarrow$ X finite $\Rightarrow$ X countable
Suppose X is infinite.
Have X bijects with its image $f(X)$ under f
so enough to show that $f(X)$ is countable.
But in $\mathbb{N}$ $\exists$ a smallest element, so can write down
$f(X)$ in increasing order so is countable. $\Leftarrow$ ✓ □

<u>Warning</u> In $\mathbb{R}$ let $X = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots\} \cup \{1\}$. X is countable.
But if we counted by "least element" would write down
$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots$ and never reach 1.
So have to take care e.g. when proving Prop 2.

Theorem 2 $\mathbb{N} \times \mathbb{N}$ is countable.



Proof 1 Define $a_1 = (1,1)$

and a_n inductively by writing

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

This does hit every point $(x,y) \in \mathbb{N} \times \mathbb{N}$ (e.g. induction on $x+y$) so have listed $\mathbb{N} \times \mathbb{N}$. □

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

is injective. □

Theorem 2' Let $A_1, A_2, A_3, \ldots$ be countable sets.

Then $A_1 \cup A_2 \cup A_3 \cup \ldots$ is countable.

Proof For each i have A_i countable, so can list A_i as

$a_{i1}, a_{i2}, a_{i3}, \ldots$ (may terminate)

Define $f: \bigcup_{n \in \mathbb{N}} A_n \to \mathbb{N}$

$x \mapsto 2^i 3^j$ where $x = a_{ij}$, least such i

(as x could be in more than one set A_i).

This is injective. □

Examples

1. $\mathbb{Q}$ is countable: $\mathbb{Q} = \mathbb{Z} \cup \frac{1}{2}\mathbb{Z} \cup \frac{1}{3}\mathbb{Z} \cup \ldots$

2) Set $\mathbb{A}$ (all algebraic numbers) is countable.

Enough to show that the set of all integer polynomials is countable as then $\mathbb{A}$ is a countable union of finite sets.

Thus enough to show that for each d, the set of all integer polynomials of degree d is countable.

But this set injects into $\mathbb{Z}^{d+1}$ $(a_d x^d + \dots + a_1 x + a_0 \mapsto (a_d, \dots, a_1, a_0))$ and $\mathbb{Z}^n$ is countable $\forall n$ ($\mathbb{Z} \times \mathbb{Z}$ countable so $\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ countable by induction).

□

A set is uncountable if it's not countable.

Theorem 3 $\mathbb{R}$ is uncountable.

Proof We'll show $(0,1)$ is uncountable.

Given $r_1, r_2, \dots$ in $(0,1)$ and $s \in (0,1)$ not on list.

For each r_n, have decimal expansion $r_n = 0.r_{n1}r_{n2}r_{n3}\dots$

$r_1 = 0.\ r_{11}\ r_{12}\ r_{13}\ \dots$

$r_2 = 0.\ r_{21}\ r_{22}\ r_{23}\ \dots$

$r_3 = 0.\ r_{31}\ r_{32}\ r_{33}\ \dots$

Define $s = 0.\ s_1\ s_2\ s_3\ \dots$ by e.g.

$$s_1 = \begin{cases} 5 & \text{if } r_{11} \neq 5 \\ 6 & \text{if } r_{11} = 5 \end{cases}$$ ensures $s \neq r_1$

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

Then s can't be on the list. $s \neq r_n$: differs in decimal digit n.

□

Remarks

1. This is called a diagonal argument (Cantor's diagonal argument)

2. $\mathbb{R}$ is uncountable and algebraic numbers are countable, so there exists a transcendental number (i.e. $\mathbb{A} \neq \mathbb{R}$).

   Indeed, "most" numbers are transcendental (i.e. $\mathbb{R} \setminus \mathbb{A}$ is uncountable).

because if $\mathbb{R} \setminus \mathbb{A}$ countable, then $\mathbb{R} = \mathbb{A} \cup (\mathbb{R} \setminus \mathbb{A})$ would be countable. □

Another uncountable set

Theorem 4 The power set of the naturals, $\mathbb{P}(\mathbb{N})$ is uncountable.

Proof Suppose $\mathbb{P}(\mathbb{N})$ is listed as $S_1, S_2, S_3, \ldots$. Let $S = \{n \in \mathbb{N} : n \notin S_n\}$

To ensure $S \neq S_1$: take $1 \in S$ if $1 \notin S_1$, $1 \notin S$ if $1 \in S_1$

To ensure $S \neq S_2$: take $2 \in S$ if $2 \notin S_2$, $2 \notin S$ if $2 \in S_2$ ...

(can continue $\forall S_n : n \in \mathbb{N}$: construct S not equal to any of the S_n).

□

Remarks

1. This is also a diagonal argument.
2. Alternatively: just inject $(0,1)$ into $\mathbb{P}(\mathbb{N})$: Given $x \in (0,1)$, write x in binary as $0.x_1x_2x_3\ldots$ (not ending with all 1s) and put $f(x) = \{n : x_n = 1\}$.

In fact our proof of Theorem 4 shows:

Theorem 5 For any set X, there is no bijection from the set X to the power set of X. (In fact: no surjection)

Proof Given any function $f : X \to \mathbb{P}(X)$ we show f is not surjective.

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

Then S does not belong to the image of f since $\forall x$ have $S \neq f(x)$ as they differ at element x.

1. Similar to Russell's paradox
2. Gives another proof that there is no universal set: if it is, then the power set is contained in it so there'd be a surjection ⚡

Example on countability: 

Let $A_i : i \in I$ be a family of pairwise disjoint open intervals.

Warnings: can't say "next interval" 

Answer Yes it is countable.

Proof 1 Each A_i contains a rational (as dense in $\mathbb{R}$) and the rationals are countable, so the family is countable. ✓ □

Proof 2 $\{i \in I : A_i \text{ has length } \geq 1\}$ countable - injects into $\mathbb{Z}$

$\{i \in I : A_i \text{ has length } \geq \frac{1}{2}\}$ again countable - injects into $\mathbb{Z}$

$\forall n$: $\{i \in I : A_i \text{ has length } \geq \frac{1}{n}\}$ again countable

Here we've written them all as a countable union of countable sets, so $\{A_i\}$ is countable. □

To show a set X is uncountable we can do one of

1. Run diagonal argument
2. Inject uncountable set into X

To show X is countable we can

1. List it (usually fiddly)
2. Inject it into $\mathbb{N}$
3. Use "countable union of countable sets is countable" usually best
4. If in or near $\mathbb{R}$, maybe consider $\mathbb{Q}$.

Intuitively, think of "A bijects with B" as saying that A and B "have the same size".

"A injects into B" as saying that "A is at most as large as B"
"A surjects to B" as saying that "A is at least as large as B"
(B nonempty)

For these to make sense, we'd want that (for $A, B \neq \emptyset$):
There exists an injection $f: A \to B$ iff $\exists$ a surjection $g: B \to A$

$\Rightarrow$ Fix $a_0 \in A$. Define $g: B \to A$ by

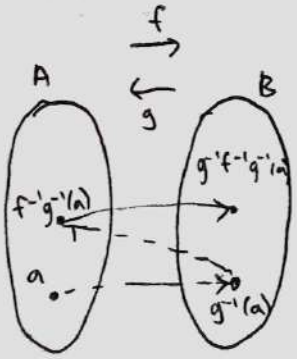
$$b \mapsto \begin{cases} \text{the unique } a \in A \text{ with } f(a) = b & \text{if it exists} \\ a_0 & \text{if not} \end{cases}$$

Then g is surjective.

$\Leftarrow$ For each $a \in A$, have some $a' \in B$ with $g(a') = a$.
(As g is surjective)
Let $f(a) = a'$ for each $a \in A$. Then f is injective. $\square$

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

Theorem 6 (Schröder - Bernstein Theorem) If $f: A \to B$ and $g: B \to A$ are injections, then $\exists$ a bijection $h: A \to B$.



Proof For $a \in A$, write $g^{-1}(a)$ for the $b \in B$ (if it exists) such that $g(b) = a$.
Similarly for $f^{-1}(b)$ where $b \in B$.

The ancestor sequence of $a \in A$ is
$g^{-1}(a)$, $f^{-1}(g^{-1}(a))$, & $g^{-1}(f^{-1}(g^{-1}(a)))$ etc.
(May terminate)

Similarly for $b \in B$

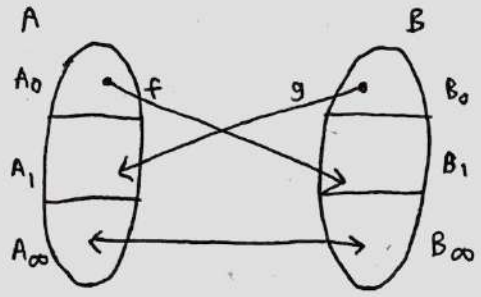
"stops in A" ↗ includes $t = 0$"

Let A_0 be $\{a \in A$: ancestor sequence stops at even time$\}$

Let A_1 be $\{a \in A$: ancestor sequence stops at odd time$\}$ ↘ "stops in B"

Let A_∞ be $\{a \in A$: ancestor sequence does not stop$\}$

Similarly for B_0, B_1, B_∞.



Then f bijects A_0 with B_1

If you start in A_0, then applying f puts you in B_1 (even → odd)

So every $b \in B$ is $f(a)$ for some $a \in A_0$.

Similarly, g bijects B_0 with A_1.

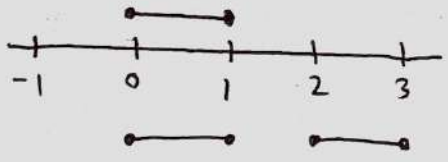
And f or g bijects A_∞ with B_∞. So the function

$h: A \to B$ with

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

is a bijection. □

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



Have injection

$f: [0,1] \to [0,1] \cup [2,3]$

e.g. $f(x) = x$

and $g: [0,1] \cup [2,3] \to [0,1]$: e.g. $g(x) = \frac{x}{3}$

an injection

so by Schröder-Bernstein they biject. □

World also be nice to have that for any sets A, B: either A injects into B or B injects into A.

This is true, but harder - see Part II "Set Theory and Logic"

Have $\mathbb{N}$, $\mathbb{P}(\mathbb{N})$, $\mathbb{P}\mathbb{P}(\mathbb{N})$, ...

Does every X inject into one of these sets?

No: e.g. $X = \mathbb{N} \cup \mathbb{P}(\mathbb{N}) \cup \mathbb{P}\mathbb{P}(\mathbb{N}) \cup \ldots$ is a countable union

Then $X' = X \cup \mathbb{P}(X) \cup \mathbb{P}\mathbb{P}(X) \cup \ldots$

Then $X'' = X' \cup \mathbb{P}(X') \cup \mathbb{P}\mathbb{P}(X') \cup \ldots$

and so on

Then $Y = X \cup X' \cup X'' \cup X''' \cup \ldots$

"and can keep going".

What happens next

Factorisation $\longrightarrow$ IB Groups, Rings and Modules

Fermat, -1 square mod p etc. $\longrightarrow$ II Number Theory

(see quadratic reciprocity)

Analysis $\longrightarrow$ IA Analysis I

Countability etc $\longrightarrow$ II Set Theory and Logic $\longleftrightarrow$

Generators

Working in $\mathbb{Z}_p^*$ (nonzero elements of $\mathbb{Z}_p$) under multiplication.

The order of $x \in \mathbb{Z}_p^*$ is the least $n \in \mathbb{N}$ with $x^n = 1$.

(Exists as $x^{p-1} = 1$).

e.g. in $\mathbb{Z}_7^*$: $2^1 = 2$, $2^2 = 4$, $2^3 = 1$ ✓ 2 has order 3

$3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$,

$3^6 = 1$ so 3 has order 6.

Say x is a generator or primitive root mod p if it has order $p-1$.

Aim $\exists$ generator g with $\mathbb{Z}_p^* = \{g, g^2, g^3, \ldots, g^{p-1} = 1\}$

i.e. $\mathbb{Z}_p^*$ is cyclic (wrt $\times$).

If x has order n, then $x^{2n} = 1$, $x^{3n} = 1$, ...

Proposition 1 If x has order n and $x^d = 1$, then n divides d.

Proof Suppose not: write $d = qn + r$ where $q \geq 0$, $0 < r < n$

Then $x^{qn+r} = 1$, $x^n = 1 \Rightarrow x^r = 1$ ✱ □

Proposition 2 Let x have order a and y have order b. If a and b are coprime, then xy has order ab.

Proof Have $(xy)^{ab} = x^{ab} y^{ab} = 1$.

Given $(xy)^d = 1$, want $ab \mid d$:

Have $x^d y^d = 1$ (Raise to power b to kill the y)

So $x^{db} = 1 \Rightarrow a \mid db$ but a, b coprime so $a \mid d$.

Similarly, $y^{da} = 1 \Rightarrow b \mid da \Rightarrow b \mid d$.

a, b coprime so $ab \mid d$ as required.

So xy has order ab. □

What if a, b are not coprime?

Proposition 3 Let x have order a and y have order b. Then $\exists$ an element of order $\text{lcm}(a, b)$.

Example first: Suppose $\text{ord}(x) = 8$, $\text{ord}(y) = 10$. Then y^2 has order 5, so xy^2 has order 40 (prop. 2).

Proof Write $a = p_1^{a_1} \cdots p_k^{a_k} q_1^{c_1} \cdots q_j^{c_j}$

$b = p_1^{b_1} \cdots p_k^{b_k} q_1^{d_1} \cdots q_j^{d_j}$

where $p_1 \cdots p_k$, $q_1 \cdots q_j$ distinct primes, $a_i \geq b_i \geq 0 \ \forall i$, $d_i \geq c_i \geq 0 \ \forall i$.

Then $x^{q_1^{c_1} \cdots q_j^{c_j}}$ has order $p_1^{a_1} \cdots p_k^{a_k}$

$y^{p_1^{b_1} \cdots p_k^{b_k}}$ has order $q_1^{d_1} \cdots q_j^{d_j}$

so their product has order $p_1^{a_1} \cdots p_k^{a_k} q_1^{d_1} \cdots q_j^{d_j}$

$= \underline{\text{lcm}(a, b)}$. □

Corollary 4 Let greatest order of all elements of $\mathbb{Z}_p^*$ be d. Then $\forall x \in \mathbb{Z}_p^*$, $\text{ord}(x)$ divides d.

Proof If not, then applying Prop. 3 would give an element of $\text{lcm}(\text{ord}(x), d) > d$. ✗

□

Remark The above all holds in any finite abelian group.

Proposition 5 In $\mathbb{Z}_p$ (p prime), a polynomial of degree k has at most k roots.

(coeff. of x^k is nonzero in $\mathbb{Z}_p$.)

Proof If polynomial f has no roots ✓

If $\exists$ a root $a \in \mathbb{Z}_p$ then write $f(x) = (x-a)\,g(x)$ where g has degree $k-1$. Now g has $\leq k-1$ roots (induction) and roots of $(x-a)\,g(x)$ are a and roots of g (p prime). □

Theorem 6 $\mathbb{Z}_p^*$ (p prime) has a generator.

Proof Let d be the greatest order of all elements of $\mathbb{Z}_p^*$: want to show that this is $p-1$.

$x^d = 1 \quad \forall x \in \mathbb{Z}_p^*$ (corollary 4)

Thus the polynomial $x^d - 1$ has $p-1$ roots, so $d \geq p-1$. □

Some things that are easy once we know $\exists$ a generator g:

1) Fermat's Little Theorem: for any $x \in \mathbb{Z}_p^*$, have $x = g^a$ for some a (def. of generator) so $x^{p-1} = (g^a)^{p-1}$ $= (g^{p-1})^a = 1^a = 1$.

2) From now on, $p > 2$.

The squares in $\mathbb{Z}_p^*$ are $g^2, g^4, g^6, g^8, \ldots, g^{p-1} = 1$ (p odd ↓ $p-1$ even)

Hence square × square = square (all even powers)

non-square × square = non-square

non-square × non-square = square by parity

3) -1 a square: have $g^{p-1/2} = -1$ as $g^{p-1} = 1$.

Thus -1 is a square iff $\frac{p-1}{2}$ is even.

4) $1 \times 2 \times 3 \times \ldots \times (p-1) = g^1 g^2 g^3 \ldots g^{p-1} = g^{p(p-1)/2}$

$= \left(g^{\frac{p-1}{2}}\right)^p = (-1)^p$ (Wilson's theorem)

5) Cubes: cubes are $g^3, g^6, g^9, \ldots$

If $p = 3k+1$ then cubes are $g^3, g^6, g^9, \ldots, g^{p-1}$

so exactly $\frac{1}{3}$ of all elements of $\mathbb{Z}_p^*$ are cubes

If $p = 3k+2$: every element is of the form g^{3n} so is a cube. (cyclic group, order $3k+1$)

Remarks proved $\exists$ generator, not how to find it. (Not even understood when 2 is a generator); not known if 2 is a generator mod p for infinitely many p (Artin's conjecture)