Numbahs & Sets

Davenport's "Higher arithmetic"

- Maths is a human activity
- We need clear language to express thoughts
- Normal language can be ambiguous
  e.g. "nothing is better than everything joy
  an egg is better than nothing
  ergo ... "
- The language of sets can be useful

$\mathbb{N} = \{1, 2, \dots, n, \dots\}$: the set of natural numbers

$3 \in \mathbb{N}$ "3 is in $\mathbb{N}$" "3 is an element of $\mathbb{N}$"

i.e. 3 is a natural number

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$: the set of integers

$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}\right\}$: the rational numbers

$\mathbb{R}$: the real numbers $\mathbb{C}$: the complex numbers

- We assume standard properties
  e.g. $a + b = b + a$, $ab = ba$ commutativity
  $a(b+c) = ab + ac$ distributivity
- A function $f : A \to B$ is a "thing" assigning to each element $a \in A$ exactly one element $f(a) \in B$.
  - We call A the domain of f
    and B the codomain of f

§ Proofs

A proof is a sequence of true statements without logical gaps, a logical argument establishing some conclusion.

We have to start somewhere.
Have agreed assumptions (axioms).

We want to proove things b/c
- We want to know they are true
- We hope to get insight into why they are true
- We might be lucky and the proof is beautiful

Examples of statements:
- there are ∞ primes of the form n^2+1
- there is always a prime between n and $2n$
- there is no computer program which will factorise an n-digit number in n^3 steps
- for every polynomial $p(x) = a_n x^n + a_0 + \cdots$ where $a_i \in \mathbb{C}$, $p(x) \neq a_0$, there exists a number $z \in \mathbb{C}$ s.t. $p(z) = 0$
- $mn = nm \quad \forall\ n, m \in \mathbb{N}$
- $2 + 2 = 4$

First: no-one knows if it's true
Second: not obvious but true
Third: no idea where to start
A counterexample might be easier

Fourth: FTA is true
Fifth: worth thinking about
Sixth: does it need proving?

Some proofs and non-proofs

Assertion $\forall\ n \in \mathbb{N}$, $n^3 - n$ is divisible by 3

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

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

Assertion if n^2 is even, so is n

"Proof" If n is even, $n = 2k$ where $k \in \mathbb{Z}$

so $n^2 = 4k^2$ which is even. □

Drivel we wanted to prove n^2 even $\Rightarrow$ n even

we proved n even $\Rightarrow$ n^2 even

Assertion if n^2 is divisible by 9 so is n

"Proof" If $n = 9k$ then $n^2 = 9(9k^2)$. □

Also drivel.

In fact the assertion is false.

"One counterexample is enough"

Assertion if n^2 even then n even

Proof Suppose on the contrary then n is not even

Then n is odd.

So $n = 2k+1$ for some $k \in \mathbb{Z}$

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

which is odd.

Contradicting the assumption that n^2 is even. □

A proof by contradiction.

Assertion the solution to $x^2 - 5x + 6 = 0$

is $x = 2 \vee x = 3$

This is actually two assertions

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

(ii) there are no other solutions

L2.1

Assertion The solution of x^2-5x+6 is $x=2$ or $x=3$

Proof (i) If $x=2 \vee x=3$
then $(x-2)=0 \vee (x-3)=0$
so $(x-2)(x-3)=0$
so $x^2-5x+6=0$

(ii) $x^2-5x+6=0$
$\Rightarrow (x-2)(x-3)=0$
so $(x-2 \vee x-3)=0$
so $x=2 \vee x=3$. □

Alternatively,

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

vital that every step is $\iff$

Assertion every positive real is ≥ 1

"Proof" Let r be the smallest positive real

Either $r<1$ or $r=1$ or $r>1$ (trichotomy)

If $r<1$ then $0<r^2<r$ (contradiction)
↑ to "r is the smallest positive real"

If $r>1$ then $0<\sqrt{r}<r$ (contradiction)

So $r=1$ "□"

Denial we don't know that there is a smallest positive real

Moral: every claim must be justified

If P and Q are both assertions, we can (but we usually don't) write

$P \wedge Q$ for "P and Q" $P \vee Q$ "P or Q"

$\neg P$ "not P"

The truth of these assertions depends on the truth of P and of Q, explained by truth table

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$P \Rightarrow Q$
f	f	f	f	t	t
f	t	f	t	t	t
t	f	f	t	f	f
t	t	t	t	f	t

L2.2

Note eg $\neg(P \wedge Q)$ equivalent to $(\neg P) \vee (\neg Q)$

(compare tables)

Also $P \Rightarrow Q$ equivalent to $(\neg P) \vee Q$

so to $Q \vee (\neg P)$

so to $(\neg Q) \Rightarrow (\neg P)$

We often use "quantifiers"

eg " for all $n \in \mathbb{N}$ ... "

$\forall x \in \mathbb{R}$ ... means for all $x \in \mathbb{R}$ ...

$\exists x \in \mathbb{R}$ ... means there exists some $x \in \mathbb{R}$ such that ...

Negating quantifiers:

$\neg(\forall x \in \mathbb{R}\ P(x))$ means $\exists x \in \mathbb{R}\ \neg P(x)$

$\neg(\exists x \in \mathbb{R}\ Q(x))$ means $\forall x \in \mathbb{R}\ \neg Q(x)$

ORDER of quantifiers matters

FTA if $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$

$a_i \in \mathbb{C}$ $a_n \neq 0$ $n \geq 1$

then $\exists\ \underset{\sim}{x} \in \mathbb{C}$ such that $P(\underset{\sim}{x}) = 0$

Proof Choose a $z \in \mathbb{C}$ which minimises $|p(z)|$

If $|p(z)| = 0$ done.

If $|p(z)| > 0$ write

$$p(z+h) = p(z) + b_1 h + b_2 h^2 + \cdots + b_n h^n$$

← expanded using binomial

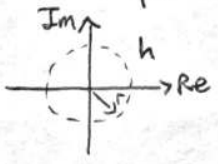
note: $b_n = a_n$

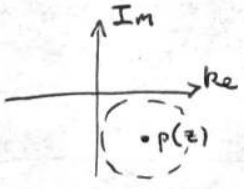
Let $\ell = \min\{ j : b_j \neq 0 \}$. ← exists, else p is const. also $b_n = a_n \neq 0$

Note $b_n = a_n \neq 0$, so ℓ is well-defined

Hence $p(z+h) = p(z) + b_\ell h^\ell + \cdots + b_n h^n$

Let $q(h) = p(z) + b_\ell h^\ell$





As h whizzes round circle radius r $q(h)$ whizzes ℓ times round circle centre $p(z)$ radius $|b_\ell| r^\ell$

L2.3

Choose r "small enough" $r \in \mathbb{R}$ $r > 0$ so that

(i) $|b_\ell| r^\ell < \frac{1}{2}|p(z)|$ → used so circle around $p(z)$ is small enough

(ii) $|b_{\ell+1}| r + \cdots + |b_n| r^{n-\ell} < |b_\ell|/2$ → used to get $q(h)$ close to $p(z+h)$

Note RHS are +ve

LHS get smaller as r gets smaller

By (i) we can choose h so that

$|q(h)| = |p(z)| - |b_\ell| r^\ell$

is closest pt nearest origin

By (ii) $|p(z+h)| \leq |q(h)| + \frac{|b_\ell| r^\ell}{2} < |p(z)|$

a contradiction. □

$|p(z+h)| \leq |q(h)| + |b_{\ell+1}||h^{\ell+1}| + |b_{\ell+2}||h^{\ell+2}| + \cdots + |b_n||h^n|$ (Δ inequality)

$= |q(h)| + |b_{\ell+1}| r^{\ell+1} + |b_{\ell+2}| r^{\ell+2} + \cdots + |b_n| r^n$ ($|h| = r$)

$= |q(h)| + r^\ell \{ |b_{\ell+1}| r + |b_{\ell+2}| r^2 + \cdots + |b_n| r^{n-\ell} \}$

$< |q(h)| + r^\ell \frac{|b_\ell|}{2}$ (by (ii))

$= |p(z)| - |b_\ell| r^\ell + \frac{1}{2}|b_\ell| r^\ell$ (by (i))

$= |p(z)| - \frac{1}{2}|b_\ell| r^\ell$

$< |p(z)|$ ☺

BUT we need to justify $\exists z$ minimising $|p(z)|$

$\exists A$ so if $|z| > A$ then $|p(z)| > |a_0| = |p(0)|$

(because $p()$ is a polynomial)

THM Analysis $|p(z)|$ is continuous and attains its minimum on the closed interval $-A \leq |z| \leq A$

we need to bound $|a_j z^j|$ as $\frac{|a_n z^n|}{2n}$

$\therefore |p(z)| \geq |a_n z_n| - |a_{n-1} z^{n-1} + \cdots + a_0|$

$> |a_n z_n| - n \cdot \frac{|a_n z^n|}{2n}$ and we happy

L3.1 §1 Sets, Functions and Relations

Sets the order of elements in a set is immaterial and elements are counted only once

e.g. if $a=1$, $b=1$, $c=2$

then $\{a,b,c\} = \{1,2\} = \{2,1\}$.

A is a subset of B, written $A \subseteq B$ or $A \subset B$, if every element of A is an element of B.

Two sets are equal if they have the same elements.

Equivalently $A = B \iff A \subseteq B \wedge B \subseteq A$.

or $\forall x \quad x \in A \iff x \in B$

In particular there is only one empty set $\emptyset$

If X is a set and P is a property of (some) elements of X we can write

$\{x \in X : P(x)\}$ or $\{x \in X \mid P(x)\}$

for the subset of X comprising those elements for which P holds.

e.g. $\{n \in \mathbb{N} : n \text{ is prime}\} = \{2,3,5,7,11,\ldots\}$.

If A and B are sets their intersection is the set

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

Their union is

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

Clearly $(A \cap B) \cap C = A \cap (B \cap C)$ etc.

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

($\notin$: is not a member)

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

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 ($x \in A$ and $x \in C$)

so $x \in A \cap B \quad \vee \quad x \in A \cap C$

hence $LHS \subseteq RHS$

argument works both ways, ergo $RHS \subseteq LHS$ and we are done. □

If X is a set, the power set

$\mathcal{P}(X)$ is the set of all subsets of X

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

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

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

$$\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots$$
$$= \{x : x \in A_n \text{ for some } n \in \mathbb{N}\}.$$

More generally if we have a collection of sets A_α indexed by I we can write

$$\bigcap_{\alpha \in I} A_\alpha = \{x \in A_\alpha \text{ for all } \alpha \in I\}$$

$$\bigcup_{\alpha \in I} A_\alpha = \{x \in A_\alpha \text{ for some } \alpha \in I\}.$$

A final operation is that of cartesian product

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

the set of ordered pairs (a,b)

Here $(a,b) = (a',b') \iff a = a'$ and $b = b'$.

(can define $(a,b) = \{a, \{a,b\}\}$).

We can extend to ordered triples etc. eg $\mathbb{R}^3 = \{(x,y,z) : \{x,y,z\} \subseteq \mathbb{R}\}$

Making new sets from old by above rules is ok.

Doesn't allow eg

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

for if it were a set Z then $Z \in Z \Rightarrow Z \notin Z \Rightarrow Z \in Z \cdots$

Russell's Paradox

Equivalent to saying the collection of all sets is not itself a set.

L3.3

Functions

A function is a thing $f: A \to B$ assigning to each element $a \in A$ exactly one element $f(a) \in B$.

Can write $a \longrightarrow f(a)$

Formally, it is a subset of $A \times B$ such that for each element $a \in A$, there is exactly one $b \in B$ with (a, b) is in the subset.

[Think: "graph" of f]

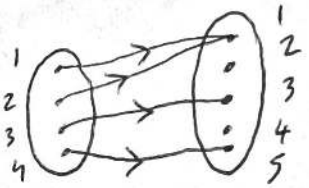
eg from $\mathbb{R}$ to $\mathbb{R}$ $\quad x \to \frac{1}{x}$ <u>not</u> a function (no $f(0)$)

$x \to \pm x$ <u>not</u> a function (not exactly one value)

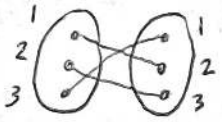
<u>examples</u>

1) $f: \mathbb{R} \to \mathbb{R} \qquad x \longrightarrow x^2$

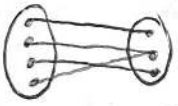
2) $f: \{1,2,3,4\} \longrightarrow \{1,2,3,4,5\}$



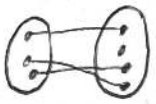
3) $f: \{1,2,3\} \longrightarrow \{1,2,3\}$



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



5) $f: \{1,2,3\} \longrightarrow \{1,2,3,4\}$



"function" means every LH dot has 1 line

A function is <u>injective</u> if $\quad a \neq a' \Rightarrow f(a) \neq f(a')$

Equivalently $\quad f(a) = f(a') \Rightarrow a = a'$

1) not injective $f(1) = f(-1)$

2) not " $f(1) = f(2)$

3) is inj.

4) not inj. $f(2) = f(4)$

5) is inj.

A function is surjective if $\forall\ b \in B \quad \exists\ a \in A \quad f(a) = b$

1) not surjective (-1 not hit)

2) not " (2 not hit)

3) is surj.

4) is surj.

5) not surj.

A function is bijective if it is injective and surjective

3) is bijective, others not

- If $f: A \to B$ is a bijection then everything is hit exactly once.

"f pairs A with B"

A permutation of A is a bijection $A \to A$.

If $f: A \to B$ and $g: B \to C$ then the composition gf or $g \circ f$ is the function $g \circ f: A \to C$ given by $a \longrightarrow g(f(a))$.

Note if $h: C \to D$ then

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

- Drop brackets

If $f: A \to B$ and $U \subseteq A$ we write $f(U) = \{b \in B : \exists u \in U \text{ s.t. } b = f(u)\}$

NOTE different use of $f(\ )$

We call $f(A)$ the image of f.

Thus f is surjective iff $f(A) = B$.

If $f: A \to B$ and $V \subseteq B$ we write $f^{-1}(V) = \{a \in A : f(a) \in B\}$.

- NOTE we did not define an inverse function $f^{-1}: B \to A$

So $f^{-1}(B) = A$ always

Let $id_A: A \to A$ be the identity map $id_A(a) = a$.

Let $f: A \to B$. Is there a map $g: B \to A$ with $gf = id_A$?

If g exists, and $a, a' \in A$ and $f(a) = f(a')$, then $gf(a) = gf(a')$

so $a = a'$. Thus f must be injective

Conversely if f is injective we can find such a g:

- if $b \in f(A)$ let $g(b) = a$ where $f(a) = b$ (this is unique)

if $b \notin f(A)$ let $g(b) =$ anything

L4.2 Is there a map $g: B \to A$ with $fg = id_B$?

We need $f(g(B)) = B$ so f must be surjective.

Conversely if f is surjective we can find such a g:

for each element $b \in B$ (pick) some $a \in A$ with $f(a) = b$
and put $g(b) = a$.

[The assertion that you can so pick is called "Axiom of Choice"]

If f is a bijection we can find a g with $fg = id_B$ $gf = id_A$.
This g is called the inverse of f written $f^{-1}: B \to A$.

A relation on a set A, call it R, specifies that some elements are "related" to some others. Formally, a relation is a subset of $A \times A$.

We write aRb rather than $(a,b) \in R$.

Examples of relations on $\mathbb{N}$

i) aRb if a, b have same final digit

2) aRb if $a|b$ $\quad 2R6 \quad 2\not R7$

3) aRb if $a \neq b$

4) aRb if $a = b = 1$

5) aRb if $|a-b| \leq 3$

6) aRb if either $a, b \geq 5$ or $a, b \leq 4$

Here are three properties of possible interest:

R is reflexive if $\forall a \in A$, aRa

R is symmetric if $\forall a, b \in A$, $aRb \Rightarrow bRa$

R is transitive if $\forall a, b, c \in A$, $aRb \wedge bRc \Rightarrow aRc$

L4.3

example	1	2	3	4	5	6
reflexive	✓	✓	x	x	✓	✓
symmetric	✓	x	✓	✓	✓	✓
transitive	✓	✓	x	✓	x	✓

Definition A relation is an equivalence relation if it is reflexive, symmetric and transitive. So 1 & 6 are equivalence relations.

examples A = deck of cards
aRb if a, b same suit

$A = \mathbb{Z} \cup \mathbb{R}$
aRb if $a - b \in \mathbb{Z}$

both equivalence relations

- In these examples, the relation partitions the set into pieces with related elements.

1) partition into classes with same final digit $0, 1, 2, \ldots, 9$

6) partition into two pieces $\{1, 2, 3, 4\}$ $\{5, 6, \ldots\}$

cards pieces clubs, diamonds, hearts, spades

$\mathbb{R}$ infinitely many pieces
↑ each piece is numbers with same fractional part

- An equivalence relation is usually written $\sim$ not R : $a \sim b$

L5.1

A <u>partition</u> of the set A is a collection of pairwise disjoint subsets (called "parts") whose union is A

N.B. $\forall y, z : y = z \vee y \cap z = \emptyset$

If $\sim$ is an equivalence relation on A the <u>equivalence classes</u> of $a \in A$ is $[a] = \{b \in A : a \sim b\}$.

e.g. i) $[423] = \{$ all numbers ending in $3\}$

cards $[8$ of hearts$] = \{$all hearts$\}$

<u>Important observation</u>: given any partition of A, there is an equivalence relation $\sim$ for which the equivalence classes are the parts of the partition.

just define $a \sim b$ if a, b in same part

<u>Theorem</u> Let $\sim$ be an equivalence relation on A. Then the equivalence classes form a partition of A.

<u>Remark</u> partitions and equivalence relations are thus "two sides of the same coin"

Ptn "global view" Eq R "local view"

<u>Proof</u> Since $\sim$ is reflexive we have $a \sim [a]$ $\forall a \in A$. Thus $\bigcup_{a \in A} [a] = A$. What remains is to show that $\forall a, b \in A$, either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

Suppose $[a] \cap [b] \neq \emptyset \Rightarrow \exists c \Rightarrow A$ s.t. $c \in [a] \cap [b]$.

Then $a \sim c$ and $b \sim c$. By symmetry, $c \sim b$.

Since $a \sim c$ and $c \sim b$, by transitivity $a \sim b$.

Let now $d \in [b]$. Then $b \sim d$.

Since $a \sim b$ and $b \sim d$, by transitivity, $a \sim d \Rightarrow d \in [a]$.

Thus if $[a] \cap [b] \neq \emptyset$ then $[b] \subseteq [a]$; similarly $[a] \subseteq [b]$.

So $[a] = [b]$.

□

L5.2

The quotient map is the map $q: A \longrightarrow [\text{equivalence classes}]$

$a \longrightarrow [a]$

e.g. q : cards $\longrightarrow$ suits

2 Division

Given $a, b \in \mathbb{Z}$, "a divides b" if $\exists c \in \mathbb{Z} : b = ac$.

We write $a|b$; "a is a factor of b"

$\pm 1, \pm b$ are always factors: other factors are proper

Theorem 1 ("Division Algorithm")

Given $a, b \in \mathbb{N}$, $\exists q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$.

Moreover, q and r are unique.

Proof Choose $q \in \mathbb{Z}$ maximal such that $qb \leq a$. Thus $(q+1)b > a$.

Thus if we write $r = a - qb$ then $0 \leq r < b$.

Suppose $a = qb + r = q'b + r'$ $\quad 0 \leq r, r' < b$.

Then $(q - q')b = r' - r$. So $b | r' - r$.

But $-b < r' - r < b$. So $q - q' = 0$ and $r' - r = 0$. $\square$

A common factor of a and b is a number $c \in \mathbb{Z}$ such that $c|a$ and $c|b$.

The highest common factor or greatest common divisor is the largest (+ve) common factor of a and b.

If d is the highest common factor we write $d = hcf(a, b)$ or $d = (a, b)$. ↗ NOT an ordered pair

How would you find the common factors of 4931 and 3795?

(Primes (a) hard)

(b) illegal

Observe if $c|4931$ and $c|3795$

$\Rightarrow c | 4931 - 3795 = 1136$

So common factors of 4931 and 3795 are also factors of 3795 and 1136.

L 5.3

Reversible:

$$c \mid 3795 \wedge c \mid 1136 \Rightarrow c \mid 3795 + 1136 = 4931$$

i.e. common factors of 4931 and 3795 are <u>exactly</u> the common factors of 3795 and 1136.

If $u, v \in \mathbb{Z}$ then $ua + vb$ is called a <u>linear combination</u> of a and b.

<u>Note</u> if $c \mid a$ and $c \mid b$ then if $u, v \in \mathbb{Z}$,

$$\left.\begin{array}{l} a = kc \\ b = \ell c \end{array}\right\} \text{ some } k, \ell \qquad \text{so } ua + vb = (uk + b\ell)c \Rightarrow c \mid ua + vb.$$

<u>Theorem</u> Let $a, b \in \mathbb{N}$. Let $d = (a, b)$. Then every common factor of a and b is a factor of d.

<u>Proof</u> Let $S = \{ ua + vb : u, v \in \mathbb{Z} \}$. Let e be the smallest positive element of S. Then $e = xa + yb$ for some $x, y \in \mathbb{Z}$. If c is a common factor of a and b, it divides e. Need only show $e \mid a$ and $e \mid b$: then $e = d$.

By the division algorithm, $\exists q, r$ with $a = qe + r$ and $0 \leq r < e$.

Thus $r = a - qe = (1 - qx)a - qyb$. Hence $r \in S$.

Since $0 \leq r < e$ and ^+e is the smallest +ve element of S, we have $r = 0$. Thus $e|a$. Symmilarly $e|b$. □

Unexpected corollary.

Corollary 3 (Bézout's Theorem)

Let $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then c is a linear combination of a, b (i.e. $\exists u, v \in \mathbb{Z}$ with $c = ua + vb$) iff $(a,b)|c$.

Proof Let $d = (a,b)$. If $c = ua + vb$, then $d|c$, since $d|a$ and $d|b$.

Conversely, suppose $d|c$, say $dk = c$ for some $k \in \mathbb{Z}$. By the proof of Theorem 2, $d = xa + yb$ for some $x, y \in \mathbb{Z}$. Then $c = kd = (kx)a + (ky)b$. □

How do we actually find d? Can we also find u, v with $d = ua + vb$?

If $a = qb + r$ then we saw that the common factors of a, b are exactly the same as the common factors of b, r.

Example $a = 57$ $b = 42$

common factors of 57 & 42	$57 = 1 \cdot 42 + 15$
$=$ " " " 42 & 15	$42 = 2 \cdot 15 + 12$
$=$ " " " 15 & 12	$15 = 1 \cdot 12 + 3$
$=$ " " " 12 & 3	$12 = 4 \cdot 3 + 0$
$=$ " " " 3 & 0	
$=$ factors of 3	$\therefore (57, 42) = 3$

This is Euclid's Algorithm

$a = q_1 b + r_1$

$b = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$\vdots$

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$

$r_{n-2} = q_n r_{n-1} + \boxed{0}$ STOP since $r_n = 0$

Eventually $r_n = 0$ happens because remainders decrease

- Algorithm works because cfs of a, b = cfs of b, r_1 = ...
  = cfs of $r_{n-1}, 0$
  = factors of r_{n-1}

Note it gives an alternative proof of Thm 2

It is fast. Eg $609953 = 466007 + 143946$ (1.)

$466007 = 3 \cdot 143946 + 34169$
$143946 = 4 \cdot 34169 + 7270$
$34169 = 4 \cdot 7270 + 5089$
$7270 = 1 \cdot 5089 + 2181$
$5089 = 2 \cdot 2181 + 727$
$2181 = 3 \cdot 727 + 0$, so $(466007, 609953) = 727$

In fact $a \geq b + r_1 > 2r_1$ so left-hand number in algorithm at least halves every two steps [hence $< \frac{1}{10}$ in 8 steps] hence number of steps is $\leq 2 \log_2 N$ which is $O(\log N)$.

- [Aside: if you do prime factorisation, you might divide a by every number up to $\sqrt{a}$ so number of steps grows as $\sqrt{a}$.
  Suppose you have a really fast machine and factorise 10-digit number in $\frac{1}{1000}$ sec. Takes me and Euclid 10 sec to do the same.

	me	(you)	
10 dig	10s	$\frac{1}{1000}$ sec	for 40 dig: (you) more than 3000 yrs]
12 dig	12s	$\frac{1}{100}$ sec	
14 dig	14s	$\frac{1}{10}$ sec	
16 dig	16s	1 sec	
20 dig	20s	100 sec	
30 dig	30s	3'5 months	

L6.3 Moreover working backwards we can write r_{n-1} as a linear combination of r_{n-3} and r_{n-2}, then of r_{n-4} and r_{n-3}, ..., then of a and b.

Example

$57 = 2\cdot 21 + 15$
$21 = 1\cdot 15 + 6$
$15 = 2\cdot 6 + 3$
$6 = 2\cdot 3$

$3 = 3(57 - 2\cdot 21) - 2\cdot 21 = 3\cdot 57 - 8\cdot 21$
$3 = 15 - 2(21 - 15) = 3\cdot 15 - 2\cdot 21$
$3 = 15 - 2\cdot 6$

$(57, 21) = 3 = 3\cdot 57 - 8\cdot 21$

Can we work out $d = ua + vb$ directly without working backwards?
A bit of thought shows we can work out each r_j as a linear combination of a, b.

Write A_n, B_n: $A_{-1} = 0$ $B_{-1} = 1$
$A_0 = 1$ $B_0 = 0$

and for $j \geq 1$ $A_j = q_j A_{j-1} + A_{j-2}$ $B_j = q_j B_{j-1} + B_{j-2}$

		A_j	B_j	
$j=-1$		0	1	$a\cdot B_{-1} - b\cdot A_{-1} = a$
$j=0$		1	0	$a\cdot B_0 - b A_0 = -b$
$j=1$	$a = q_1 b + r_1$	q_1	1	$aB_1 - bA_1 = r_1$
$j=2$	$b = q_2 r_1 + r_2$	$q_2 A_1 + A_0$	$q_2 B_1 + B_0$	$aB_2 - bA_2 = -r_2$

$aB_1 - bA_1 = a - bq_1 = r_1$

say $aB_k - bA_k = r_k(-1)^{k+1}$, $aB_{k-1} - bA_{k-1} = r_{k-1}(-1)^k$

then $aB_{k+1} - bA_{k+1} = q_{k+1}\left[aB_k - bA_k\right] + \left[aB_{k-1} - bA_{k-1}\right]$

$= q_{k+1}(-1)^{k+1} r_k + (-1)^k r_{k-1}$

$= (-1)^k \left[r_{k-1} - q_{k+1} r_k\right] = (-1)^{k+2} r_{k+1}$ ☺

L.7.1

$j=3$ $\quad r_1 = q_3 r_2 + r_3$ $\qquad\qquad\qquad\qquad$ $aB_3 - bA_3 = r_1 - q_3 r_2 = r_3$

$j=4$ $\quad r_2 = q_4 r_3 + r_4$ $\quad q_4 A_3 + A_2 \quad q_4 B_3 + B_2 \quad aB_4 - bA_4 = q_4 r_3 - r_2 = -r_4$

$\uparrow \qquad \uparrow \qquad \uparrow$

j^{th} line $= q_j (j-1)^{th}$ line $+ (j-2)^{th}$ line

Hence $\boxed{aB_j - bA_j = (-1)^{j-1} r_j}$

e.g.

	0 1
	1 0
$57 = 2\cdot 21 + 15$ →	2 1
$21 = 1\cdot 15 + 6$ →	3 1
$15 = 2\cdot 6 + 3$ →	[8 3]
$6 = 2\cdot 3$ →	19 7

$(57,21) = 3 = 3\cdot 57 - 8\cdot 21$

	0 1
	1 0
$83 = 2\cdot 30 + 23$	2 1
$30 = 1\cdot 23 + 7$	3 1
$23 = 3\cdot 7 + 2$	11 4
$7 = 3\cdot 2 + 1$	[36 13]
$2 = 2\cdot 1 + 0$	83 30

$(83,30) = 1 = (-13)(83) + (36)(30)$

so $\boxed{aB_{n-1} - bA_{n-1} = (-1)^{n(-2)} r_{n-1} = \pm \text{hcf}(a,b)}$

Now $aB_n - bA_n = 0$

so $\boxed{\dfrac{a}{b} = \dfrac{A_n}{B_n}}$

Suggest looking at $A_n B_{n-1} - B_n A_{n-1}$

more generally

$$A_j B_{j-1} - B_j A_{j-1}$$

$$= (q_j A_{j-1} + A_{j-2}) B_{j-1} - (q_j B_{j-1} + B_{j-2}) A_{j-1}$$

$$= -(A_{j-1} B_{j-2} - B_{j-1} A_{j-2})$$

$$= (-1)^2 (A_{j-2} B_{j-3} - B_{j-2} A_{j-3})$$

$$\cdots = (-1)^j (A_0 B_{-1} - B_0 A_{-1}) = (-1)^j$$

In particular $\boxed{\text{hcf}(A_j, B_j) = 1}$.

How do we interpret the other A_j, B_j?

$$\frac{57}{21} = 2 + \frac{15}{21} \qquad \frac{21}{15} = 1 + \frac{6}{15} \qquad \frac{15}{6} = 2 + \frac{3}{6} \qquad \frac{6}{3} = 2$$

$$\therefore \frac{57}{21} = 2 + \frac{1}{\frac{21}{15}} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{2}}}$$

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \; \frac{1}{q_n}}}$$

This is called a continued fraction.

Hence $\dfrac{A_n}{B_n} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \; \frac{1}{q_n}}}$.

What about, say, A_3, B_3?

let $\dfrac{c}{d} = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3}}$

If we apply Euclid to c, d we get quotients q_1, q_2, q_3 and stop after 3 steps.

We'd get the same values of A_1, A_2, A_3 as in the original calc^n for a, b.

since $\frac{A_n}{B_n} = \frac{a}{b}$ before

Then $\dfrac{A_3}{B_3} = \dfrac{c}{d} = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3}}$ so is the result of truncating the original cont^d fraction.

The fractions $\dfrac{A_1}{B_1}, \dfrac{A_2}{A_2}, \ldots, \dfrac{A_n}{B_n}$ are called the convergents to $\dfrac{a}{b}$.

[A_j, B_j unexaminable]

Primes

Definition $p \in \mathbb{N}$ is prime if $p > 1$ and the only factors of p are ± 1 and $+p$ (in $\mathbb{Z}$).

Every number can be written as a product of primes – for if $n \in \mathbb{N}$ is not itself prime, write as product $n = ab$. If either a or b is not prime, write $a = cd$, then $n = cdb$, and so on until n is a product of primes.

Theorem There are infinitely many primes

Proof (Euclid)

Let $p_1, \dots, p_k$ be primes.

Let $N = p_1 p_2 \cdots p_k + 1$.

Now $p_1 \nmid N$, else $p_1 \mid N - p_1 \cdots p_k = 1$.

Likewise none of $p_2, \dots, p_k$ divide N.

But N is a product of primes.

So there must be a prime other than $p_1, \dots, p_k$. □

2nd Proof (Erdős)

Let $p_1, \dots, p_k$ be primes.

Any number which is a product of these primes has the form

$$p_1^{j_1} p_2^{j_2} \cdots p_k^{j_k} = m^2 p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k} \quad \text{where } i_x \in \{0, 1\}$$

Let M be any number. If a number $\leq M$ is of this form, then $m^2 \leq M \Rightarrow m \leq \sqrt{M}$ and there are 2^k numbers of the form $p_1^{i_1} \cdots p_k^{i_k}$

So there are at most $\sqrt{M} \times 2^k \leq M$ numbers of this form.

If $M > \sqrt{M} \times 2^k$, i.e. $M > 4^k$, then there must be some number $\leq M$ not of this form, so it has a prime factor not among $p_1, \dots, p_k$. □

Note Euclid says this number has all prime factors outside our list shows k^{th} prime is $< 2^{2^k}$.

- Erdős says some number $< M$ has some factor not in the list. Shows k^{th} prime is $< 4^k$.

In fact k^{th} prime $\sim k \log k$ (prime number theorem)

Can a number have more than one prime factorisation?

Our previous argument to show a prime factorisation exists does not give uniqueness
- two different people might follow different tracks and end up with different lists of primes

- Clearly $21 = 3 \cdot 7$ unique

What about $295869 ? = 3 \cdot 7 \cdot 73 \cdot 193$

Is this fraction $\frac{6701}{9049} \stackrel{?}{=} \frac{40099}{54151}$ Does $9049 \times 40099 \stackrel{?}{=} 6701 \times 54151$

$362855851 \quad 362865851$

There are "arithmetical systems" (permitting addition, substraction, multiplication) where factorization is not unique

- e.g. even numbers $= \{2, 4, 6, 8, \ldots\}$

"primes" are $2 \times$ odd number $2, 6, 10, 14, \ldots$

$$60 = 2 \cdot 30 = 6 \cdot 10$$

This example had no 1 but next does

e.g. $\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

primes? can show ✓

- Theorem If $a|bc$ and $(a, b) = 1$ then $a|c$.

Remark if $(c, b) = 1$, we say "a, b are coprime"

Proof Since $(a,b)=1$, by Euclid / Bézout there exist $u, v \in \mathbb{Z}$ with $ua+vb=1$. Then $uac+vbc=c$. Since $a|bc$, $a|$LHS.

$\therefore a|c$. □

Corollary If p is prime and $p|bc$, then $p|b$ or $p|c$.

Proof Since (p,b) is a factor of p, we have $(p,b)=1$ or $(p,b)=p$.

If $(p,b)=p$ then $p|b$. If $(p,b)=1$, by Theorem, $p|c$. □

Theorem (Fundamental Theorem of Arithmetic)

Every natural number is expressible as a product of primes in exactly one way.

That is, if $p_1 \cdots p_k = q_1 \cdots q_l$ where $p_1, \ldots, q_l$ are primes then $k=l$ and $q_1, \ldots, q_l$ are $p_1, \ldots, p_k$ in some order.

Proof 1 Let $p_1 \cdots p_k = q_1 \cdots q_l$. Then $p_1 | q_1(q_2 \cdots q_l)$. By Corollary applied to p_1, either $p_1|q_1$ or $p_1|q_2 \cdots q_l$. If $p_1|q_1$ then $p_1=q_1$ since q_1 is prime.

So either $p_1|q_1 \iff p_1=q_1$ or $p_1|q_2 \cdots q_l$. In second case either $p_1=q_2$ or $p_1|q_3 \cdots q_l$. $\therefore p_1 =$ one of the q_j. By relabeling the q_j we may assume $p_1=q_1$. Then $p_2 \cdots p_k = q_2 \cdots q_l$. So p_2 is one of the other q_j.

$\therefore k=l$ and p_i are q_j in some order. □

Remark we already showed every number is expressible in at least one way so the proof needs only to show uniqueness.

Proof 2 (without Euclid)

Suppose FTA false. Let $N = p_1 \cdots p_k = q_1 \cdots q_l$ be the smallest number with more than one factorisation.

Notice $p_i \neq$ any q_j (else divide both sides by that number to get smaller counterexample)

So we may assume $p_1 < q_1$. Consider $N - p_1 q_2 \cdots q_l = (q_1 - p_1) q_2 \cdots q_l$.

This is a positive integer smaller than N, so it has a unique prime factorisation.

One way to get such a fac^n is to take the prime fac^n of $p_1 - p_1$ together with $q_2, \cdots, q_\ell$. So this must be the only fac^n.

But $N = p_1 q_2 \cdots q_\ell = p_1(p_2 \cdots p_k - q_2 \cdots q_\ell)$. This gives another way to factorise: p_1 together with the prime fac^n of $(p_2 \cdots p_k - q_2 \cdots q_\ell)$. This must give the same fac^n. Only way is if p_1 is a prime factor of $q_1 - p_1$. But then $p_1 | q_1$. □

§3. Modular Arithmetic

Definition if $a, b \in \mathbb{Z}$ have the same remainder after division by m, we say that a and b are congruent modulo m that is

$$a \equiv b \pmod m \quad \text{means} \quad m | a - b$$

e.g $9 \equiv 0 \pmod 3$ $\qquad 11 \equiv 16 \pmod 5$

by definition if $d | m$ and $a \equiv b \bmod m$ then $a \equiv b \bmod d$

e.g. $21 \equiv 11 \pmod{10} \Rightarrow 21 \equiv 11 \pmod 5$

observe that $\equiv \pmod m$ is an equivalence relation. The set of equivalence classes is often written $\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$.

e.g. $\mathbb{Z}_3 = \{[0], [1], [2]\} = \left\{ \begin{matrix} \{\cdots, -3, 0, 3, \cdots\}, \{\cdots, -2, 1, 4, \cdots\}, \\ \{\cdots, -1, 2, 5, \cdots\} \end{matrix} \right\}$

$\sqrt{M} \cdot 2^k < M$
if $M > 4^k$

$a \equiv b \pmod m$ means $m \mid b-a$

Note if $a \equiv b \pmod m$ and $u \equiv v \pmod m$

then $m \mid (a-b)+(u-v) = (a+u)-(b+v)$

$m \mid (a-b)u + b(u-v) = au - bv$

thus $a + u \equiv b + v \pmod m$

$au \equiv bv \pmod m$

So we can do arithmetic $\pmod m$

Example Show that $2a^2 + 3b^3 = 1$ has no solution $a, b \in \mathbb{Z}$

Proof if there is a solution then $2a^2 \equiv 1 \bmod 3$

$2 \cdot 0^2 \equiv 0$, $2 \cdot 1^2 \equiv 2$, $2 \cdot 2^2 \equiv \not 2$

so there is no solution. □

Notice that all odd primes are either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$.

Example There are infinitely many primes $\equiv 3 \pmod 4$ i.e. $\equiv -1 \pmod 4$.

Proof Let $p_1, \dots, p_k$ be a list of primes $\equiv -1 \pmod 4$

Let $N = 4p_1 \cdots p_k - 1$. Then $N \equiv -1 \pmod 4$.

Now N is a product of primes $N = q_1 \cdots q_\ell$.

Since each $p_i \nmid N$, no q_j is a p_i. Moreover no $q_j = 2$.

If $q_j \equiv 1 \pmod 4$ for all j, then $N = q_1 \cdots q_\ell \equiv (1)^\ell \equiv 1 \pmod 4$ contradicting $N \equiv -1 \pmod 4$. So some q_j must be $\equiv -1 \pmod 4$. Hence there is a prime of this kind other than $p_1, \dots, p_k$. □

(How does this prove fail to adapt to show infinitely many primes $\equiv 1 \pmod 4$?)

Example solve $7x \equiv 2 \pmod{10}$

We note $3 \cdot 7 \equiv 1 \pmod{10}$ so $3 \cdot 7 \cdot x \equiv 3 \cdot 2 \pmod{10}$

i.e. $x \equiv 6 \pmod{10}$.

we "divided" by 7

We can't "divide by 2": there's no u with $2u \equiv 1 \pmod{10}$

Definition u is a unit modulo m if there exists v such that $uv \equiv 1 \pmod{m}$

Theorem u is a unit modulo m iff $(u,m) = 1$.

Proof Suppose u is a unit and let $d = (u,m)$. Let $uv \equiv 1 \pmod{m}$. Since $m \mid uv-1$, $d \mid uv-1$, and $d \mid u$ so $d \mid 1$ i.e. $(u,m) = 1$.

Conversely suppose $(u,m) = 1$. Then $\exists\, v, w \in \mathbb{Z}$ such that $uv + mw = 1$.
So $uv \equiv 1 \pmod{m}$. □

(importantly) we can find v efficiently by Euclid's algorithm.

Corollary If $(a,m) = 1$ then the congruence $ax \equiv b \pmod{m}$ has a unique solution. [Means if x, x' are solutions then $x \equiv x' \pmod{m}$]. In particular there is a unique inverse u, $au \equiv 1 \pmod{m}$.

Proof Let u be same inverse $au \equiv 1 \pmod{m}$ given by the theorem.
Then $a(ub) = aub \equiv b \pmod{m}$ so $x \equiv ub \pmod{m}$ is a solution to it.
If $ax' \equiv b \pmod{m}$, then multiply by u, $x' \equiv uax' \equiv ub \pmod{m}$. □

What if $ax \equiv b \pmod{m}$ and $(a,m) = d > 1$?
Then $m \mid ax-b$ so $d \mid ax-b$ and $d \mid a$ so $d \mid b$ if there is a solution.
Conversely, if $d \mid b$, then $d \mid m$ i.e. $m = m'd$, similarly $a = a'd$, $b = b'd$ and

$$\begin{aligned} ax \equiv b \pmod{m} &\iff ax - b = km \text{ for some } k \in \mathbb{Z} \\ &\iff da'x - db' = kdm' \quad " \\ &\iff a'x - b' = km' \quad " \\ &\iff a'x \equiv b' \pmod{m'} \end{aligned}$$

Note $(a', m') = 1$.

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

L9.3 Multiple Moduli

- Observe $x \equiv 5 \pmod{12} \Rightarrow \begin{cases} x \equiv 1 \pmod 4, \\ x \equiv 2 \pmod 3. \end{cases}$

Is the converse true? I.e. does

$x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$ imply $x \equiv 5 \pmod{12}$?

Inspect: $x \equiv 1 \pmod 4$: 1 (5) $9 \pmod{12}$

$x \equiv 2 \pmod 3$: 2 (5) 8 $11 \pmod{12}$

Theorem (Chinese Remainder Theorem)

- Let $(m,n) \equiv 1$ and $a, b \in \mathbb{Z}$. Then there is a unique solution $\pmod{mn}$ to the simultaneous congruences $x \equiv a \pmod m$ and $x \equiv b \pmod n$.

[Ie there is a solution x, and y is a solution iff $x \equiv y \pmod{mn}$]

Proof Since $(m,n) = 1$ we can find $u, v \in \mathbb{Z}$ with $um + vn = 1$.

Note $vn \equiv 1 \pmod m$ and $um \equiv 1 \pmod n$.

Let $x = umb + vna$. Then $x \equiv vna \equiv a \pmod m$

$x \equiv umb \equiv b \pmod n$.

- Moreover $y \equiv a \pmod m$ and $y \equiv b \pmod n$.

$\Leftrightarrow y \equiv x \pmod m$ and $y \equiv x \pmod n$

$\Leftrightarrow m \mid y - x$ and $n \mid y - x$

* $\Leftrightarrow mn \mid y - x$ since $(m,n) = 1$

$\Leftrightarrow y \equiv x \pmod{mn}$. □

* $\Rightarrow$ justified by FTA or say $y - x = km$ because $n \mid y - x$

and $n \mid km$. $(n,m) = 1 \Rightarrow n \mid k$ (by earlier theorem)

$\therefore mn \mid y - x$

-

CRT $(m,n)=1$ then $\forall\ a,b$

$\exists$ unique (mod mn) $\quad x \equiv a \pmod m$

$\quad\quad x \equiv b \pmod n$

Remark 1) Shows congruence (mod mn) is equivalent to two congruences (mod m) and (mod n). Can be used either way round.

2) Can be extended to more than two moduli.

3) The CRT gives a bijection between $c \in \{0,1,\dots,mn-1\}$ and pairs $(a,b) \in \{0,\dots,m-1\} \times \{0,\dots,n-1\}$ given by $a \equiv c \pmod m$ and $b \equiv c \pmod n$.

Note in this bijection $c=1$ corresponds to $a=b=1$ (because it works)

also c is a unit (mod mn) iff a (mod m), b (mod n) both units.

For if c is a unit then $\exists\ u$ s.t. $cu \equiv 1 \pmod{mn}$, so $au \equiv cu \pmod m$ but $cu \equiv 1 \pmod m$. Likewise $bu \equiv cu \equiv 1 \pmod n$ so a,b both units.

Conversely if a,b both units $\quad \exists\ u : au \equiv 1 \pmod m$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \exists\ v : bv \equiv 1 \pmod n$

By CRT $\exists\ w \quad w \equiv u \pmod m,\ w \equiv v \pmod n$.

Then $cw \equiv au \pmod m \equiv 1 \pmod m$, and also

$cw \equiv bv \pmod n \equiv 1 \pmod n$.

Hence $cw \equiv 1 \pmod{mn}$, so c is a unit.

Definition (Euler's totient function)

We denote by $\phi(m)$ the number of integers a, $1 \le a \le m$ such that $(a,m)=1$, i.e. a is a unit (mod m).

So $\phi(1)=1$.

It follows from the above discussion that ϕ is multiplicative, i.e.

$$\phi(mn) = \phi(m)\,\phi(n) \quad \text{if} \quad (m,n)=1.$$

Clearly if p is prime then $\phi(p) = p-1$ and more generally

- $\phi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$.

Thus if $m = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$ (distinct p_i)

then $\phi(m) = \phi(p_1^{k_1})\,\phi(p_2^{k_2}) \cdots \phi(p_\ell^{k_\ell})$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right) p_2^{k_2}\left(1-\frac{1}{p_2}\right) \cdots p_\ell^{k_\ell}\left(1-\frac{1}{p_\ell}\right)$$

$$\therefore \phi(m) = m \prod_{p \mid m} \left(1-\frac{1}{p}\right).$$

- $\phi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$ (check)

Alternative proof later (by ind-excl).

Note that if a, b both units (mod m) so is ab; for if $au \equiv bv \equiv 1$ then $abuv \equiv 1$. Hence units form a multiplicative group of order $\phi(m)$.

Let p be a prime. Then $1, 2, \ldots, p-1$ are units. The units come in pairs whose product is 1, plus some elements that are self-inverse i.e. $x^2 \equiv 1$.

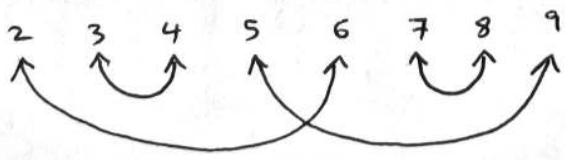
- Now $x^2 \equiv 1 \pmod p \iff p \mid x^2-1 = (x-1)(x+1)$,

$\iff p \mid x-1$ or $p \mid x+1$, * ⇒ requires corollary of FTA

$\iff x \equiv \pm 1 \pmod p$.

Thus $1, -1$ are the only self-inverse elements. The others come in pairs.

e.g. $p = 11$



Theorem (Wilson's Theorem): $(p-1)! \equiv -1 \pmod p$ iff p is prime.

- Proof $(p-1)!$ is the product of $\frac{p-3}{2}$ pairs of inverse elements together with 1 and $p-1$. □

Theorem (Fermat's Little Theorem) Let p be a prime. Then $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$. Equivalently, $a^{p-1} \equiv 1 \pmod p$ if $p \nmid a$.

Proof 1 The numbers $\{1, \dots, p-1\}$ are units $(\bmod p)$ so they form a group. So $a^{p-1} \equiv 1$. (Lagrange's Theorem) □

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

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

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

But $(p-1)!$ is a product of units, hence is a unit, so $a^{p-1} \equiv 1 \pmod p$. □

Proof 3 If $0 < k < p$ then $\binom{p}{k} \equiv 0 \pmod p$. So if $a, b \in \mathbb{Z}$ then

$$(a+b)^p = \binom{p}{0}a^p b^0 + \binom{p}{1}a^{p-1}b^1 + \cdots + \binom{p}{p}a^0 b^p$$
$$\equiv a^p + b^p \pmod p.$$

Then $1^p \equiv 1$, $2^p \equiv (1+1)^p \equiv 1^p + 1^p \equiv 2$,

$3^p \equiv 2^p + 1^p \equiv 3$, and so on... □

Remark Clearly 2nd form of theorem implies the first. First implies the second because if $a \not\equiv 0$ then a is a unit.

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

Proof Let $U = \{x \in \mathbb{N} : 0 < x < m, (x, m) = 1\}$ be the $\phi(m)$ numbers $< m$, coprime to m. Since a is a unit, $ax \equiv ay$ iff $x \equiv y$. Writing $U = \{u_1, u_2, \dots, u_{\phi(m)}\}$ then $au_1, au_2, \dots, au_{\phi(m)}$ are $u_1, u_2, \dots, u_{\phi(m)}$ in some order. So $a^{\phi(m)} z \equiv z$ where $z \equiv u_1 u_2 \cdots u_{\phi(m)}$. z is a unit so $a^{\phi(m)} \equiv 1 \pmod m$. □

L11.1 Squares $1^2, 2^2, \dots, (p-1)^2$ are squares (mod p). If $a^2 \equiv b^2 \pmod p$

then $p \mid a^2 - b^2 = (a-b)(a+b)$

- so $p \mid a-b$ or $p \mid a+b$ (by FTA)

so $a \equiv \pm b \pmod p$

So every number which is a non-zero square is the square of exactly two numbers.

So there are $\frac{p-1}{2}$ squares – we call them quadratic residues.

Eg mod 7

$1 \equiv 1^2 \equiv 6^2 \qquad 2 \equiv 3^2 \equiv 4^2 \qquad 4 \equiv 2^2 \equiv 5^2$

so 1, 2, 4 are squares and 3, 5, 6 are not

- -1 is not a square (mod 7)

-1 is a square (mod 13)

Recall Wilson's theorem

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots \left(\tfrac{p-1}{2}\right)\left(-\tfrac{p-1}{2}\right) \cdots (-3)(-2)(-1)$$

$$\equiv (-1)^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}!\right)^2$$

So if $p \equiv 1 \pmod 4$ so $p = 4k+1$, $k \in \mathbb{N}$ then

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

Thus if $p \equiv 1 \pmod 4$ then -1 is a quadratic residue.

Suppose $p \equiv -1 \pmod 4$ ie $p = 4k+3$, $k \in \mathbb{N}$

If -1 is a quadratic residue then $\exists\, z : z^2 \equiv -1 \pmod p$

But then Fermat's Theorem says $1 \equiv z^{p-1} \equiv z^{4k+2} \equiv (z^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1$

a contradiction.

We have proved the following

- Theorem Let p be an odd prime. Then -1 is a square if and only if

$p \equiv 1 \pmod 4$

Example There are infinitely many primes $\equiv 1 \pmod 4$

Proof Let $p_1, \dots, p_k$ be a list of primes $\equiv 1 \pmod 4$.

Let $N = (2p_1 \cdots p_k)^2 + 1$. N is a product of some primes $q_1, \dots, q_\ell$ none of which is 2 or $p_1, \dots, p_k$. Now for each prime q_j, $N \equiv 0 \pmod{q_j}$ so $(2p_1 \cdots p_k)^2 \equiv -1 \pmod{q_j}$. Thus $q_j \equiv 1 \pmod 4$. Hence there are primes $\equiv 1 \pmod 4$ not in our list. □

If $p = 4k+3$ we can compute square roots using Fermat. Suppose a is a qr : $a \equiv z^2$ say. Then $a^{2k+2} \equiv z^{4k+4} \equiv z^{p-1} \cdot z^2 \equiv z^2 \equiv a$.

Thus $\pm a^{k+1}$ are square roots of a.

Note we can compute powers efficiently by repeated squaring

eg $a^{37} = a^{100101_2} = a^{32} a^4 a^1 = (((((a^2)^2)^2)^2)^2)^2 (a^2)^2 a$

Number of operations is $\propto$ to # digits in exponent.

Suppose now that a is a square (mod n) where $n = pq$; p, q prime.

Then a is a square (mod p) and also (mod q). So there exists s with $(\pm s)^2 \equiv a \pmod p$ and there exists t with $(\pm t)^2 \equiv a \pmod q$.

By CRT we get four square roots of a (mod n) corresponding to the 4 choices $\pm s, \pm t$. [eg if $c \equiv -s \pmod p$ $c \equiv t \pmod q$ then $c^2 \equiv a \pmod n$]

Eg $4 \equiv (\pm 2)^2 \equiv (\pm 5)^2 \pmod{21}$

Tossing a coin over the phone

Alice and Boris wish to toss a coin fairly over the phone.

A: chooses two 100-digit primes $p, q \equiv 3 \pmod 4$

tells Boris the product $n = pq$

B: picks u coprime to n, computes $a \equiv u^2 \pmod{n}$, tells a to A

A: computes the four roots $\pm u, \pm v$ of $a \pmod{n}$ (corresponding to s,t $-s,-t$ and $s,-t$ $-s,t$)

picks a pair, either $\pm u$ or $\pm v$, tells B

B: if A says $\pm u$, B says "you win"
if A says $\pm v$, B says "you lose"

This is all feasible because it's possible to find primes with near certainty (by random Fermat-like tests) and the rest: powers, hcf, CRT, etc are feasible because of Euclid.

Can Boris cheat? If A says $\pm u$ and B says "you lose" he must produce $\pm v$ as evidence. Knowing both $\pm u$ and $\pm v$ is equivalent to knowing how to factorise n. (Certainly if he can factorise n he can find $\pm u, \pm v$, same as A.

Conversely if he knows $\pm u, \pm v$ then $u^2 \equiv v^2 \pmod{n}$

ie $n \mid (u-v)(u+v)$

but $n \nmid u-v$, $n \nmid u+v$

so wlog $p \mid u-v$ and $q \mid u+v$

then compute $p = (n, u-v)$ and $q (n, u+v)$.)

<u>But</u> it is thought to be too hard to factorise n.

Public Key Cryptography

Let us agree to write text messages as sequences of numbers

e.g. A – Z = 00 – 25
! = 26 etc.

I wish for people to be able to send me messages in encrypted form so I can decrypt them but no bad guy (who knows the encryption scheme) who is listening can decrypt.

The RSA scheme (Rivest, Shamir, Adleman)

[HMG knew it before]

I think of two large primes p, q. Let $n = pq$. Pick e coprime to $\phi(n)$ which is $(p-1)(q-1)$. Work out d with $de \equiv 1 \pmod{\phi(n)}$. Publish the pair n, e. To send me a message (i.e. a sequence of numbers) chop into numbers $M < n$ send me $M^e \pmod n$.

How do I find M? Take $(M^e)^d \equiv M^{k\phi(n)+1} \equiv M \pmod n$.

How can a bad guy find M? Finding $\phi(n)$ is as hard as factorising n. (if he finds ϕ then p, q are roots of $x^2 - (n+1-\phi)x + n = 0$).

It is believed factorisation is hard. (No proof known)

Not known if RSA can be broken without factorisation.

§4 Counting and integers

"In Cambridge $\exists$ two people with the same number of hairs"

Pigeonhole Principle: Given $(m-1)n + 1$ pigeons in n pigeonholes, some pigeonhole contains $\geq m$ pigeons

Let X be a set. For each subset $A \subset X$, define the **indicator function** of A as $i_A : X \longrightarrow \{0, 1\}$ (sometimes called the characteristic function χ_A)

$$x \longrightarrow \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$$

Note that $i_A = i_B \iff A = B$.

- $i_X = 1_X$ (i.e. $\forall x \ 1(x) = 1$)

$i_{\bar{A}} = 1 - i_A$ $(\bar{A} = X \setminus A)$

$i_{A \cap B} = i_A i_B$

We have $\overline{A \cup B} = \bar{A} \cap \bar{B}$ (De Morgan's Law), so

$$i_{A \cup B} = 1 - i_{\overline{A \cup B}} = 1 - i_{\bar{A} \cap \bar{B}} = 1 - i_{\bar{A}} i_{\bar{B}}$$
$$= 1 - (1 - i_A)(1 - i_B) = i_A + i_B - i_A i_B.$$

- $i_{A \setminus B} = i_{A \cap \bar{B}} = i_A i_{\bar{B}} = i_A (1 - i_B) = i_A - i_A i_B.$

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

Pf: $i_{LHS} = i_A i_{B \cup C} = i_A (i_B + i_C - i_B i_C) = i_A i_B + i_A i_C - i_A i_B i_C$

$i_{RHS} = i_{A \cap B} + i_{A \cap C} - i_{A \cap B} i_{A \cap C} = i_A i_B + i_A i_C - i_A i_B i_A i_C = i_{LHS}$

since $i_A^2 = i_A$.

$i_{A \triangle B} = i_A + i_B - 2 i_A i_B \equiv i_A + i_B \pmod 2$

- $i_{(A \triangle B) \triangle C} \equiv (i_A + i_B) + i_C \pmod 2$
$\equiv i_A + (i_B + i_C)$

We can find the sizes of finite sets using indicators:

$|A| = \sum_{x \in X} i_A(x)$ (↗ size of A)

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

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

●

Principle of Inclusion - Exclusion

Let $A_1, \dots, A_n$ be subsets of the finite set X.

$$|\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \cdots$$

$$+ (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Equivalently $|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|$

Remark Two are equivalent because $|A_1 \cup \cdots \cup A_n| = |X| - |\bar{A}_1 \cap \cdots \cap \bar{A}_n|$.

Proof: $i_{\bar{A} \cap \cdots \cap \bar{A}_n} = i_{\bar{A}_1} i_{\bar{A}_2} \cdots i_{\bar{A}_n} = (1 - i_{A_1})(1 - i_{A_2}) \cdots (1 - i_{A_n})$

$$= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i} i_{A_j} - \sum_{i<j<k} i_{A_i} i_{A_j} i_{A_k} + \cdots + (-1)^n i_{A_1} i_{A_2} \cdots i_{A_n}$$

$$= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i \cap A_j} - \sum_{i<j<k} i_{A_i \cap A_j \cap A_k} + \cdots + (-1)^n i_{A_1 \cap A_2 \cap \cdots \cap A_n}$$

Thus $|\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n| = \sum_{x \in X} i_{\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n}$

$$= \sum_{x \in X} 1(x) - \sum_{x \in X} \sum_i i_{A_i}(x) + \sum_{x \in X} \sum_{i<j} i_{A_i \cap A_j}(x)$$

$$- \cdots + \sum_{x \in X} (-1)^n i_{A_1 \cap A_2 \cap \cdots \cap A_n}(x)$$

(Note $\sum_x \sum_{i<j} i_{A_i \cap A_j}(x) = \sum_{i<j} \sum_x i_{A_i \cap A_j}(x)$)

$$= \sum_{x \in X} 1(x) - \sum_i \sum_{x \in X} i_{A_i}(x) + \sum_{i<j} \sum_{x \in X} i_{A_i \cap A_j}(x)$$

$$- \cdots + \sum_{x \in X} (-1)^n i_{A_1 \cap A_2 \cdots \cap A_n}(x)$$

$$= |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|. \quad \square$$

L13.1 Example: How many numbers are there ≤ 200 and coprime to 110?

Let $X = \{1, \dots, 200\}$, $A_1 = \{x : 2 \mid x\}$, $A_2 = \{x : 5 \mid x\}$, $A_3 = \{x : 11 \mid x\}$?

- Want $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3|$.

$|A_1| = \lfloor \frac{200}{2} \rfloor = 100$ $\quad |A_2| = \lfloor \frac{200}{5} \rfloor = 40$ $\quad |A_3| = \lfloor \frac{200}{11} \rfloor = 18$ ← round down

$|A_1 \cap A_2| = \lfloor \frac{200}{10} \rfloor = 20$ $\quad |A_1 \cap A_3| = \lfloor \frac{200}{22} \rfloor = 9$ $\quad |A_2 \cap A_3| = \lfloor \frac{200}{55} \rfloor = 3$

$|A_1 \cap A_2 \cap A_3| = \lfloor \frac{200}{110} \rfloor = 1$

Ans $= 200 - 100 - 40 - 18 + 20 + 9 + 3 - 1 = 73$

- Alternative proof of formula for $\phi(m)$:

$m = p_1^{k_1} \cdots p_\ell^{k_\ell}$ $\quad p_i$ distinct

Let $X = \{1, \dots, m\}$, $A_j = \{x : p_j \mid x\}$

Want $\phi(m) = |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_\ell|$. Now $|A_j| = m/p_j$, and

$|A_i \cap A_j \cap A_k| = m/p_i p_j p_k$ etc.

So $\phi(m) = m - \sum_i \frac{m}{p_i} + \sum_{i<j} \frac{m}{p_i p_j} - \sum_{i<j<k} \frac{m}{p_i p_j p_k} + \cdots$

$= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)(\cdots)\left(1 - \frac{1}{p_\ell}\right)$. □

How many subsets of $\{1, 2, \dots, n\}$ are there?

There are $2 \times 2 \times \cdots \times 2 = 2^n$ ways to choose. Equivalently, there are 2^n functions

(1 chosen? 2 in/out?)

from $\{1, \dots, n\} \to \{0, 1\}$. Define: There are $\binom{n}{r}$ subsets of $\{1, \dots, n\}$

of size r. So by definition $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

("n choose r")

more generally,

Binomial Theorem $(a+b)^n = \binom{n}{0}a^n b^0 + \cdots + \binom{n}{r}a^{n-r}b^r + \cdots + \binom{n}{n}a^0 b^n$.

● **Proof** $(a+b)^n = \underbrace{(a+b)(a+b)(\cdots)(a+b)}_{n \text{ times}}$ Get sum of all terms, products from each bracket. $a^{n-r}b^r$ comes from choosing b from r brackets, and there are $\binom{n}{r}$ ways to do it. □

$\binom{n}{r}$ is called a "binomial coefficient"

Some identities

● $\binom{n}{r} = \binom{n}{n-r}$ choosing r to keep is the same as choosing $n-r$ to throw away

$\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ Pascal's identity

We choose r people from $n+1$, of whom 1 has red hair.

RHS: choose then (r from $n+1$)

LHS: choices including red + choices not including

Given that $\binom{n}{0} = \binom{n}{n} = 1$ we can construct Pascal's triangle

●
```
          1
        1   1
      1   2   1
    1   3   3   1      <- (3 r)
  1   4   6   4   1    <- (4 r)
```

$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$ Both sides count pairs of subsets Y, Z where $Y \subset Z$, $|Y| = r$, $|Z| = k$.

LHS chooses Z then chooses Y inside Z.

RHS chooses Y first then chooses $Z \setminus Y$ from outside.

● $\binom{a}{r}\binom{b}{0} + \binom{a}{r-1}\binom{b}{1} + \cdots + \binom{a}{0}\binom{b}{r} = \binom{a+b}{r}$ "Vandermonde's convolution"

Choose r people from a women and b men. RHS does this

L13.3 LHS distinguishes choices by number of women picked $\binom{a}{r-2}\binom{b}{2}$ pick $r-2$ women, 2 men

A grasshopper stocks n kinds of fruit. In how many ways can we ~~to~~ make a bag of r fruit?

If we are allowed only one of each kind, Ans $= \binom{n}{r}$. What if $r=4$ and 2 apples, 1 plum, 1 grape. Then Ans $= \binom{n+r-1}{r}$. There is a bijection between the possible bags of fruit and the binary strings of length $n+r-1$ with r 0s and $(n-1)$ 1s.

$n=5$
$r=8$

0 0 0 1 | 0 0 | 1 1 | 0 0 | 1 | 0

3 type 1, 2 type 2, 0 type 3, 2 type 4, 1 type 5

What is the numerical value of $\binom{n}{r}$? There are $n(n-1)\cdots(n-r+1)$ of choosing r elements, one by one, in order. Each subset of size r is picked in $r!$ factorial ways by this method. So $n(n-1)\cdots(n-r+1) = \binom{n}{r} r!$

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}$$

We write $x^{\underline{r}}$ for the polynomial $x(x-1)\cdots(x-r+1)$

"x to the r falling"

So $\binom{n}{r} = \frac{n^{\underline{r}}}{r!}$. Multiplying Vandermonde by $r!$ gives

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

"falling binomial theorem"

L14.1

Consider the number of derangements (ways to put n letters into n envelopes so that no letter goes into the right envelope).

- Let X = all $n!$ ways to put letters into envelopes.

For each envelope i, $i = 1, \dots, n$, let $A_i = \{x \in X : x \text{ puts letter } i \text{ in env. } i\}$.

We want $|\bar{A}_1 \cap \dots \cap \bar{A}_n|$.

$|A_i| = (n-1)!$ $\qquad$ $|A_i \cap A_j| = (n-2)!$

$|A_i \cap A_j \cap A_k| = (n-3)!$ etc.

So $|\bar{A}_1 \cap \dots \cap \bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \dots$

- $= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \dots$

$= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}\right)$

$\approx \frac{n!}{e}$

Well-ordering and induction

Several proofs used statements such as "smallest / largest integer such that ..."

e.g. Division algorithm, proof of hcfs

- or involved a sequence of operations "... and so on"

e.g. Euclid, the A_j / B_j, every number is a product of primes, and others

We need to think about what we are doing.

(Weak) Principle of induction

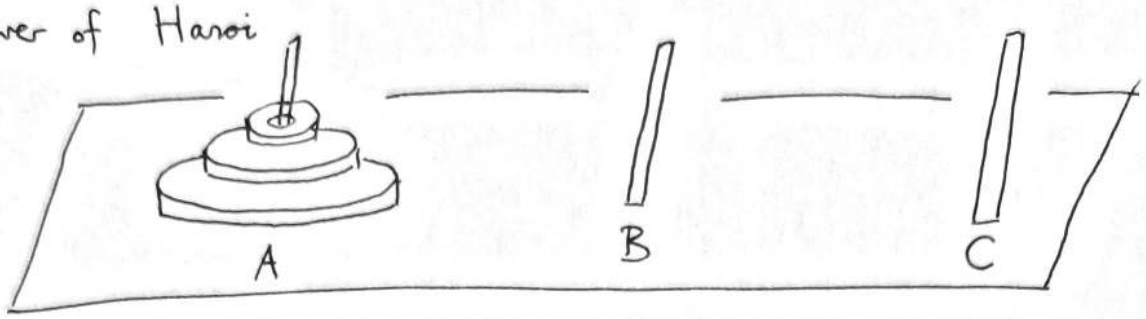
Let $P(n)$ be a statement about the number $n \in \mathbb{N}$.

Suppose that (i) $P(1)$ is true

and that (ii) $\forall n \in \mathbb{N}$, if $P(n)$ is true then $P(n+1)$ is true.

- Then $P(n)$ is true $\forall\, n \in \mathbb{N}$.

Example Tower of Hanoi



Aim: move rings to peg B

Rules: one ring at a time
never have small ringer under larger ring

Claim: needs exactly $2^n - 1$ moves (no more and no less)

Proof: Let $P(n)$ be "n rings needs exactly $2^n - 1$ moves"

$P(1)$ is clearly true.

Suppose we have $n+1$ rings. We can move n rings to C, bottom ring to B, then all rings from C to B. Assuming $P(n)$ twice, this needs $\leq (2^n - 1) \times 2 + 1$ $= 2^{n+1} - 1$ moves. So $\leq 2^{n+1} - 1$ moves needed.

Can we use fewer? We must move the bottom ring. To expose it requires $\geq 2^n - 1$ by $P(n)$. At some later time bottom ring moves to B. To move remaining rings to B requires $\geq 2^n - 1$ by $P(n)$. So need $2^{n+1} - 1$.

Hence $P(n) \Rightarrow P(n+1)$. Thus $P(n)$ is true $\forall n \in \mathbb{N}$ by WPI. □

Claim All numbers are equal

"Proof" Let $P(n)$ be "if $\{a_1, \ldots, a_n\}$ is a set of n numbers then $a_1 = a_2 = \cdots = a_n$".

$P(1)$ true.

Suppose have $\{a_1, \ldots, a_{n+1}\}$. By $P(n)$ on $\{a_1, \ldots, a_n\}$ $a_1 = \cdots = a_n$.

By $P(n)$ on $\{a_2, \ldots, a_{n+1}\}$ $a_2 = \cdots = a_{n+1}$.

So $a_1 = \cdots = a_{n+1}$ so $P(n) \Rightarrow P(n+1)$

"□"

Argument fails to prove P(2)

MORAL check small cases carefully

- Claim Inclusion-Exclusion is correct.

Proof: Let $P(n)$ be $|A_1 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots$

For $n=1$, $P(n)$ is true trivially.

Also $P(2)$ is true by inspection.

Suppose we have $A_1, \ldots, A_{n+1}$. Let $B_i = A_i \cap A_{n+1}$ $\quad 1 \le i \le n$.

Notice that $B_i \cap B_j = A_i \cap A_j \cap A_{n+1}$,

$B_i \cap B_j \cap B_k = A_i \cap A_j \cap A_k \cap A_{n+1}$.

- Now $|A_1 \cup \cdots \cup A_{n+1}| = |A_1 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup \cdots \cup A_n) \cap A_{n+1}|$

by $P(2)$, giving $= |A_1 \cup \cdots \cup A_n| + |A_{n+1}| - |B_1 \cup \cdots \cup B_n|$.

Applying $P(n)$ to both $|A_1 \cup \cdots \cup A_n|$ and $|B_1 \cup \cdots \cup B_n|$,

$$|A_1 \cup \cdots \cup A_{n+1}| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots$$

$$+ |A_{n+1}|$$

$$- \sum_{i=1}^{n} |B_i| + \sum_{1 \le i < j \le n} |B_i \cap B_j| - \cdots$$

-

$$= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \cdots + |A_{n+1}|$$

$$- \sum_{i=1}^{n} |A_i \cap A_{n+1}| + \sum_{1 \le i < j \le n} |A_i \cap A_j \cap A_{n+1}| - \cdots$$

Thus $P(n) \Rightarrow P(n+1)$. Since $P(1)$ is true, $P(n)$ true $\forall n \in \mathbb{N}$. □

Note induction gives insight into Tower of Hanoi but not I.E.

- WPI not quite what we need for "every number is a product of primes"

Strong principle of induction

- Let $P(n)$ be a statement about $n \in \mathbb{N}$. Suppose

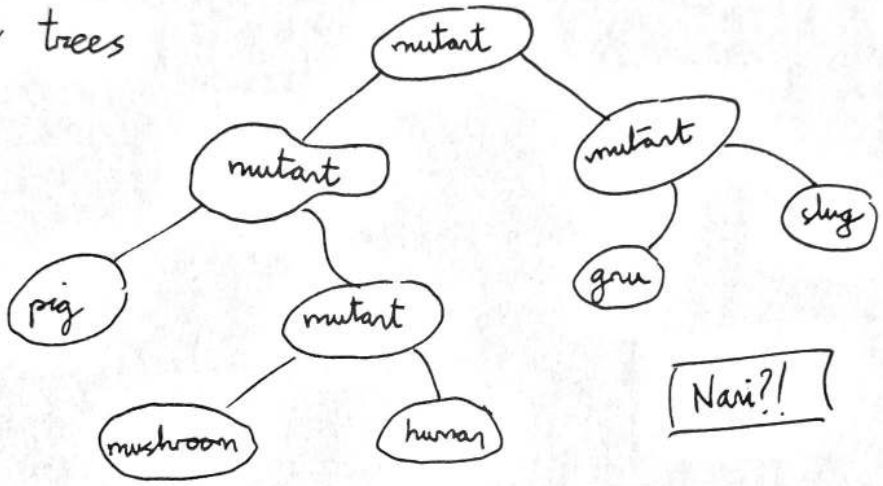
  (i) $P(1)$ true

  (ii) $\forall\, n \in \mathbb{N}$, if $P(k)$ true $\forall\, k < n$, then $P(n)$ true.

Then $P(n)$ is true $\forall\, n \in \mathbb{N}$.

Note (i) is redundant, as it is covered by (i). We keep it for clarity.

Example evolutionary trees



$P(n)$: " $n-1$ mutants yields n animals"

Proof Given a tree with n animals*

remove the top mutant, to get two evolutionary trees with n_1, n_2, animals where $n_1 + n_2 = n$ and $n_1, n_2 \geq 1$.

- If $P(k)$ true $\forall\, k < n$, we can assume $P(n_1)$ & $P(n_2)$.

So total mutants $= (n_1 - 1) + 1 + (n_2 - 1) = n - 1$, so $P(n)$ holds.

Hence by SPI $P(n)$ holds $\forall\, n \in \mathbb{N}$.

!

Theorem: WPI is equivalent to SPI

Proof: clearly SPI $\Rightarrow$ WPI

[either observe $(P(1) \wedge \dots \wedge P(n)) \Rightarrow P(n+1)$ implies $P(n) \Rightarrow P(n+1)$

or any proof using WPI could use SPI]

To show WPI $\Rightarrow$ SPI suppose (i) and (ii) of SPI hold. We want to show $P(n)$ true for all n using WPI.

Let $Q(n)$ be "$P(1) \wedge P(2) \wedge \dots \wedge P(n-1)$". Note $Q(1)$ is vacuously true. Also, $Q(2)$ is true. Given $Q(n)$, by (ii) of SPI, $P(n)$ is true.

Hence $Q(n+1)$ is true, i.e. $Q(n) \Rightarrow Q(n+1)$.

By WPI, $Q(n)$ is true for all n. Hence $P(n)$ is true for all n. □

A partial order on a set is a relation that is

reflexive,

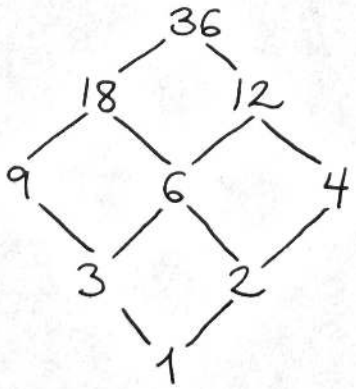
antisymmetric ($aRb \wedge bRa \Rightarrow a=b$),

and transitive.

We often write $a \leq b$ instead of aRb. Not every pair of elements need be comparable.

Example on $\mathbb{N}$, write "$a \leq b$" if $a \mid b$

factors of 36



If $\forall a, b$ either $a \leq b$ or $b \leq a$ we say the order is total.
(combined with antisymmetry this is trichotomy)

A total order is called a well-order if every non-empty subset S has a minimal element (i.e. $\exists m \in S : x < m \Rightarrow x \notin S$)

$\mathbb{Q}$ is totally ordered but not well-ordered:

$S = \{q : q > 0\}$ has no minimal element.

Well-ordering principle $\mathbb{N}$ is well-ordered, i.e. every non-empty subset has a minimal element.

Theorem SPI is equivalent to WOP

Proof To show WOP implies SPI suppose (i) and (ii) of SPI hold. We want to show $P(n)$ true $\forall n$, using WOP.

Suppose that $P(n)$ is not true $\forall n$. Then $C = \{n : \neg P(n)\} \neq \emptyset$. ($C$ is set of counterexamples.) By WOP, C has a minimal element m. (m is a minimal counterexample.) Now $\forall k < m$, $k \notin C$ (by minimality of m). So $P(k)$ is true $\forall k < m$. By (ii) of SPI, $P(m)$ is true. Contradiction. So SPI holds.

To show SPI $\Rightarrow$ WOP, let $S \subset \mathbb{N}$ and suppose S has no minimal element. We want to show $S = \emptyset$ using SPI. Let $P(n)$ be "$n \notin S$". Certainly $1 \notin S$ (else 1 would be minimal), so $P(1)$ is true.

Suppose $P(k)$ true $\forall k < n$. Then $k \notin S$ $\forall k < n$. So $n \notin S$, else it would be minimal. Thus $P(n)$ is true. So (ii) of SPI holds. Then $P(n)$ is true $\forall n$, ie. $S = \emptyset$. □

WOP enables us to prove $P(n)$ true for all n as follows:

- if not, there is a minimal counterexample;
- try to derive a contradiction.

Examples evolutionary trees

every number a product of primes

- if not, let n be a minimal counterexample.
  either n is prime (contradiction), or $n = ab$
  where both a, b are products of primes.

"all numbers are interesting"

"Proof" Certainly 1, 2, 3 are interesting. If claim is false, by WOP, there is a minimal counterexample, m. So m is the smallest uninteresting number. What could be more interesting than that? Contradiction.

Note that a totally ordered set is well ordered iff there is no infinite descending chain $x_1 > x_2 > \cdots > x_n > \cdots$

[If there is such a chain, then the set $\{x_1, \ldots, x_n, \ldots\}$ has no minimal element. Conversely, if $S \neq \emptyset$ has no minimal element, pick $x_1 \in S$, pick $x_2 \in S$ with $x_2 < x_1$ because x_1 is not minimal, pick $x_3 < x_2$, and so on. Get $x_1 > x_2 > \cdots > x_n > \cdots$]

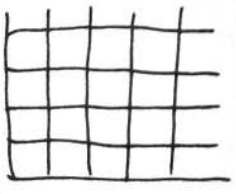
Example The Ackermann function $a : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}$ defined by

$a(0,n) = n+1$,

$a(m,0) = a(m-1, 1)$ if $m > 0$,

$a(m,n) = a(m-1, a(m, n-1))$ if $m, n > 0$.

Is this well defined? The lexicographic or dictionary order on $\mathbb{N}_0^2$ is $(u,v) \leq (x,y)$ if $u < x$ or $(u = x$ and $v \leq y)$.

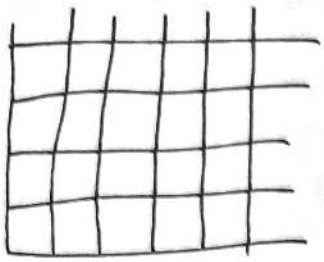


notice $a(m,n)$ is defined in terms of $a(u,v)$ for $(u,v) < (m,n)$

Hence definition is good if the ordering is well-ordered.

It is well-ordered, for if $(u_1, v_1) > (u_2, v_2) > \cdots$ where an infinite descing chain, then $u_1 \geq u_2 \geq \cdots$ By WOP only finitely many are distinct. So $u_k = u_{k+1} = \cdots$ Then $v_k > v_{k+1} > \cdots$ contradicting WOP. □

Need to know WPI, SPI, WOP



Note There are infinite ascending chains here, not the whole of the set
— No such chain is the whole —

Peano Arithmetic

Can we characterise the integers $\mathbb{N}$?

Peano (1892) defined $\mathbb{N}$ in the following way:
(Dedekind did same in 1888)

- $\mathbb{N}$ is a set with a special element 1 and a map $S: \mathbb{N} \to \mathbb{N}$ (successor) such that:

(i) $\forall n,\ S(n) \neq 1$

(ii) $\forall n, m \quad n \neq m \Rightarrow S(n) \neq S(m)$

(iii) if $A \subset \mathbb{N}$, $1 \in A$, and, $\forall n \in A$, $S(n) \in A$, then $A = \mathbb{N}$.

Note (iii) is equivalent to WPI.

Now write 2 for $S(1)$, 3 for $S(2)$, ... etc.

- Crucial fact: if $n \neq 1$, $\exists m \in \mathbb{N}$ s.t. $S(m) = n$

Define addition: by induction

$k + 1 = S(k)$, ~~$k + x =$~~ $k + S(m) = S(k + m)$

multiplication:

$k \times 1 = k$, $k \times S(m) = k \times m + k$

order:

$n < m$ if $\exists k \in \mathbb{N}$ s.t. $n + k = m$

- Long tedious verification of properties

§5. The Reals

- The central characteristic of $\mathbb{N}$ is induction. Formally, construct via Peano's axioms.

$\mathbb{Z}$ is obtained from $\mathbb{N}$ by allowing subtraction.

$\mathbb{Q}$ ... $\mathbb{Z}$ ... division.

Formally, we can construct $\mathbb{Q}$ from $\mathbb{Z}$ as follows:

define a relation $\sim$ on $\mathbb{Z} \times \mathbb{N}$ by

$$(a,b) \sim (c,d) \text{ iff } ad = bc$$

- Check $\sim$ is an equivalence relation

Let $\mathbb{Q}$ be the set of equivalence classes

We write $\frac{a}{b}$ for $[(a,b)]$.

Need to check we can define $+, \times, <$ on $\mathbb{Q}$ to make it a <u>totally ordered field</u>.

(a) $\mathbb{Q}$ is an additive abelian group with identity 0

(b) $\mathbb{Q} \setminus \{0\}$ is a multiplicative abelian group with identity 1

- (c) mult. is distributive over add, i.e. $a(b+c) = ab + ac$

(a) - (c) make $\mathbb{Q}$ into a field

(d) There is an order relation $\leq$ on $\mathbb{Q}$ that is reflexive, antisymmetric, transitive

(e) which is <u>total</u>, i.e. $\forall\ p, q \in \mathbb{Q}$ either $p \geq q$ or $q \geq p$

(d) - (e) make $\mathbb{Q}$ a totally ordered set

(f) the order respects the field, i.e. $\forall\ p, q, r \in \mathbb{Q}$

$$p \leq q \Rightarrow p + r \leq q + r$$

- and $p \leq q,\ 0 \leq r \Rightarrow pr \leq qr$

A totally ordered field satisfies (a) - (f)

Note in a totally ordered field:

$$0 = (-1)(1+(-1)) = -1 + (-1)^2$$

so $1 = (-1)^2$.

Also $0 < 1$ for otherwise $1 < 0$ (trichot.)

so $1 + (-1) < 0 + (-1) \Rightarrow 0 < -1$

then $0 < -1,\ 0 < -1 \Rightarrow 0 = 0^2 < (-1)^2 = 1$ contradiction.

Observe integers (mod p) $0, 1, \dots, p-1$ form a field, but it cannot be ordered: else we would have

$0 < 1$, so $0 + 1 < 1 + 1$ i.e. $1 < 2$,

likewise $2 < 3, 3 < 4, \dots$

$p - 1 < p = 0$

by transitivity $0 < 0$ contradiction.

Note $\mathbb{Q}$ is dense: if $p, q \in \mathbb{Q}$ with $p < q$ then $\exists\, r \in \mathbb{Q} : p < r < q$

e.g. $r = \frac{p+q}{2}$.

But we cannot solve equations in $\mathbb{Q}$.

Theorem: there is no rational $q \in \mathbb{Q}$ with $q^2 = 2$

Proof: suppose not, and that $\left(\frac{a}{b}\right)^2 = 2$ where b is as small as possible.

Hence $(a, b) = 1$ and $a^2 = 2b^2$.

① Since a^2 is even, then a is even (see start of lectures). So $a = 2c$, then $2c^2 = b^2$, so b is even, contradicting $(a, b) = 1$. $\square_1$

② We know b is a product of primes. Let $p \mid b$. Then $p \mid a^2$. By theorem, $p \mid a$. Contradiction. $\square_2$

③ We have $\frac{a}{b} = \frac{2b}{a}$. So for every $u, v \in \mathbb{Z}$,

$$\frac{a}{b} = \frac{au + 2bv}{bu + av}.$$ Put $u = -1$, $v = 1$.

Then $\frac{a}{b} = \frac{2b - a}{a - b}$. Since $a < 2b$, RHS is a fraction whose square is 2 and has a smaller denominator. $\square_3$

④ As in proof 3 but choose u, v with $bu + av = 1$.

Thus $\frac{a}{b}$ is an integer! $\square_4$

L17.1 To prove $\nexists q \in \mathbb{Q} \quad q^2 = 72$

Proof 1 : very hard

Proof 3 : need division algorithm

Proofs 2 & 4 immediate but use Bézout

So we can split the rationals into two bits with "a gap":

$$\{ q \in \mathbb{Q} : q < 0 \text{ or } q^2 < 2 \} \cup \{ q \in \mathbb{Q} : q > 0 \text{ and } q^2 > 2 \}$$

The real numbers fill this gap.

But we need to avoid relying on intuition.

e.g. is $0.999\ldots = 1$?

Def^n The number $s \in \mathbb{R}$ is a <u>least upper bound</u> for the set $S \subset \mathbb{R}$ if (i) s is an upper bound for S i.e. $x \in S \Rightarrow x \leq s$

(ii) if t is an upper bound for S, then $s \leq t$

The central property of $\mathbb{R}$ is the assumption

"$\mathbb{R}$ is a totally ordered field containing $\mathbb{Q}$ and where

<u>Axiom:</u> Every non-empty set of real numbers that has an upper bound has a least upper bound."

By definition (ii) if least upper bound exists it is unique.

We write $s = \sup S$ the <u>supremum</u> of S

Note $\mathbb{Q}$ doesn't satisfy the axiom e.g. $\{ q \in \mathbb{Q} : 0 < q^2 < 2 \}$ has no sup

[Formally: it can be shown that there is at most one object satisfying the properties of $\mathbb{R}$.

We can construct a set $\mathbb{R}$ from $\mathbb{Q}$ having these properties:

We let $\mathbb{R}$ be the set of all partitions $L \cup R$ of $\mathbb{Q}$ where

$\forall l \in L, r \in R, \; l \leq r$

Inject $\mathbb{Q}$ into $\mathbb{R}$ as $q \to \{ x \in \mathbb{Q} : x \leq q \} \cup \{ x > q \}$.

L17.2 Show $\mathbb{R}$ has stated properties. "Dedekind cuts"

There are other ways to build $\mathbb{R}$ from $\mathbb{Q}$.]

Examples Let $a \leq b \in \mathbb{R}$

Define $[a,b] = \{ x \in \mathbb{R} : a \leq x \leq b \}$ "closed interval"

$(a,b) = \{ \text{"} : a < x < b \}$ "open interval"

$[a,b)$ and $(a,b]$ "half-open".

Let $S = [0,1]$. Then $S \neq \emptyset$. Also, 2 is an upper bound, since $x \leq 2$ $\forall\ x \in S$. Hence $\sup S$ exists. Note 1 is an upper bound also. If $t < 1$ then t is not an upper bound because $1 \in S$. Hence $\sup S = 1$.

Let $S = (0,1)$. Then $S \neq \emptyset$ and 1 is an upper bound. If $t < 1$ then if $t \leq 0$ then $t < \frac{1}{2} \in S$, and if $t > 0$ then $t < \frac{1+t}{2} \in S$, so t is not an upper bound for S. Hence $\sup S = 1$.

If S has a maximum element then $\sup S = \max S$, but $\sup S$ can exist when $\max S$ does not: $\sup S \notin S$.

Theorem (Axiom of Archimedes)

Given $r \in \mathbb{R}$ there exists $n \in \mathbb{N}$ with $n > r$.

Proof If not, every $n \in \mathbb{N}$ is less than or equal to r. Since $\mathbb{N} \neq \emptyset$, $s = \sup \mathbb{N}$ exists. Since s is the least upper bound for $\mathbb{N}$, $s-1$ is not an upper bound for $\mathbb{N}$. So there is an $n \in \mathbb{N}$ with $n > s-1$. But then $n+1 > s$, contradicting s being an upper bound for $\mathbb{N}$. □

Notice every non-empty set of reals which is bounded below has a greatest lower bound or infimum, because $-S = \{ -x : x \in S \}$ is non-empty and bounded below and

L17.3 $\inf S = -\sup(-S)$.

Corollary $\inf\{\frac{1}{n} : n \in \mathbb{N}\} = 0$

Proof Clearly 0 is a lower bound. If $t > 0$ then by Archimedes $\exists\, n \in \mathbb{N}$ with $n > \frac{1}{t}$, so $t > \frac{1}{n}$ and t is not a lower bound. □

Theorem + corollary show there are no "infinitely large" or "infinitely small" reals.

We can show $\mathbb{Q}$ is dense in $\mathbb{R}$, i.e. given $r < s$ real numbers, $\exists\, q \in \mathbb{Q}$ where $r < q < s$.

Assume $0 < r$. By Corollary, $\exists\, n \in \mathbb{N}$ with $\frac{1}{n} < s - r$.

By the Ax of Arch, $\exists\, N \in \mathbb{N}$ with $N > s$.

Let $T = \{k \in \mathbb{N} : k/n \geq s\}$. Then $Nn \in T$ so $T \neq \emptyset$.

By WOP T has a least element m. Put

$q = \frac{m-1}{n}$. Since $m - 1 \notin T$, $q < s$. If $q \leq r$, then

$\frac{m}{n} = q + \frac{1}{n} < s$. contradiction So $r < q < s$. □

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

Proof: $S = \{r \in \mathbb{R} : r^2 \leq 2\}$. Then $0 \in S$ so $S \neq \emptyset$, and

3 (say) is an upper bound for S.

Hence $\sup S = x$ exists, and $0 \leq x \leq 3$.

Suppose $x^2 < 2$. Let $0 < t < 1$. $(x+t)^2 = x^2 + 2xt + t^2$

$\leq x^2 + 6t + t$

$= x^2 + 7t$.

Pick $t < \frac{2 - x^2}{7}$. Then $(x+t)^2 < 2$, so $x + t \in S$ contradicting \$ x being an upper bound for S.

Suppose $x^2 > 2$. Let $0 < t < 1$. Then

$(x-t)^2 = x^2 - 2xt + t^2 \geq x^2 - 6t$.

Pick $t < \frac{x^2 - 2}{6}$. Then $(x-t)^2 > 2$, contradicting

L17.4

x being the least upper bound.

By trichotomy, $x^2 = 2$. □

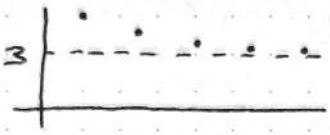
L18.1 Note proof works just as well in $\mathbb{Q}$ except for "sup S exists"

- **Sequences** A sequence is a function $\mathbb{N} \to \mathbb{R}$.

If $a : \mathbb{N} \to \mathbb{R}$ we usually write $a_1, a_2, \ldots$ etc instead of $a(1), a(2), \ldots$

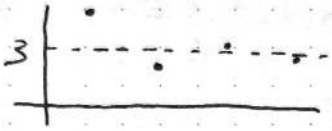
What does it mean for a sequence to tend to a limit?

examples $a_n = 3 + \frac{1}{n}$



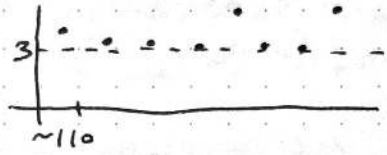
would like $a_n \to 3$

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



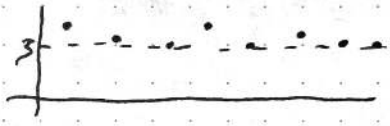
still want $a_n \to 3$

- $a_n = \begin{cases} 3 + \frac{1}{n} & \text{if } n \text{ prime} \\ 4 & \text{otherwise} \end{cases}$



would like $a_n \not\to 3$

$a_n = \begin{cases} 3 + \frac{1}{n} & \text{if } n \text{ not prime} \\ 3 + \frac{46}{n} & \text{otherwise} \end{cases}$



would like $a_n \to 3$

Def^n The sequence $(a_n)_{n=1}^{\infty}$ tends to the limit $\ell \in \mathbb{R}$ as n tends to infinity if,

for every $\varepsilon > 0$,

- there exists $N \in \mathbb{N}$,

such that for all $n > N$,

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

Symbolically,

$\forall \varepsilon > 0 \ \exists N \ \forall n > N \ |a_n - \ell| < \varepsilon$

We also write "$a_n \to \ell$ as $n \to \infty$"

or "$\lim_{n \to \infty} a_n = \ell$"

or "a_n converges to ℓ"

If there is a limit ℓ but it's not specified we just say "a_n converges".

- "Diverge" means "does not converge"

examples $a_n = 1 - \frac{1}{n}$

given $\varepsilon > 0$ choose $N > \frac{1}{\varepsilon}$ (use Archimedes)

if $n > N$, $|a_n - 1| = \frac{1}{n} < \varepsilon$

Thus $a_n \to 1$

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

given $\varepsilon > 0$ pick $N > \frac{1}{\varepsilon}$

if $n > N$, $|a_n - 0| \leq \frac{1}{n} < \varepsilon$

hence $a_n \to 0$

The definition of $a_n \not\to \ell$ is therefore

$$\exists \varepsilon > 0 \; \forall N \; \exists n > N \; |a_n - \ell| \geq \varepsilon$$

e.g. $$a_n = \begin{cases} 1 & n \text{ odd} \\ -1 & n \text{ even} \end{cases}$$

let $\varepsilon = \frac{1}{2}$ if $\ell \geq 0$ then $\forall N$, if $n > N$ and n even, then $|a_n - \ell| > \varepsilon$, so $a_n \not\to \ell$

if $\ell < 0$ then $\forall N$ if $n > N$ and n is odd then $|a_n - \ell| > \varepsilon$ so $a_n \not\to \ell$

Hence this sequence diverges.

A sequence is bounded if there is some real B such that $|a_n| \leq B$ for all n.

Notice a convergent sequence is bounded: for if $a_n \to \ell$ then $\exists N$ s.t. $\forall n > N$ $|a_n - \ell| < 1$

so $$|a_n| \leq \max\{|a_1|, |a_2|, \ldots, |a_N|, |\ell| + 1\}$$

The following is used constantly.

Theorem Every bounded monotonic sequence converges

L18.3 ("Monotonic means increasing or decreasing.
(a_n) is increasing if $a_{n+1} \geq a_n \ \forall n$)

Proof: Suppose (a_n) is increasing.

The set $\{ a_n : n \geq 1 \}$ is non-empty and bounded above, since the sequence is bounded above, and so has a supremum l, say.

Given $\varepsilon > 0$, then $l - \varepsilon$ is not an upper bound for the set, so there is some N with $a_N > l - \varepsilon$. Since (a_n) is increasing, $a_n > l - \varepsilon$ for all $n > N$. Thus $l - \varepsilon < a_n \leq l$ for all $n > N$. Hence for all $n > N$, $|a_n - l| < \varepsilon$ which is equivalent to $a_n \to l$. Decreasing case similar. □

Remarks 1) $a_n = n$ is increasing and not bounded (in fact it diverges)

2) Theorem is actually equivalent to Axiom of sups

Something like $a_2, a_3, a_6, a_9, \ldots$ is a subsequence.
Formally, a subsequence is $a_{g(n)}$ where $g : \mathbb{N} \to \mathbb{N}$ is strictly increasing.

Theorem: Every sequence has a monotonic subsequence

Proof: Call a_k a high point if $a_k \geq a_m \ \forall m > k$.
If there are infinitely many high points, they form a decreasing subsequence.
If not, there exists some N so that $\forall n > N$, a_n is not a high point. Pick a $n_1 > N$. It's not a high point, so pick a_{n_2}, $n_2 > n_1$, $a_{n_2} \geq a_{n_1}$, pick a_{n_3}, $n_3 > n_2$, $a_{n_3} \geq a_{n_2}$ and so on forever obtaining an increasing subsequence. □

$S_n = \sum_{n=1}^{n} a_n$. If $S_n \to S$ we say $\sum_{n=1}^{\infty} a_n = S$.

examples $a_n = r^n$ where $|r| < 1$ (geometric series)

$$S_n = r \times \frac{1-r^n}{1-r} \longrightarrow \frac{r}{1-r} \quad \text{since } r^n \to 0$$

i.e. $\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$

$a_n = \frac{1}{n}$ harmonic series

$$S_{2^k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^k}$$

$$\geqslant 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + 4\left(\frac{1}{8}\right) + \cdots + 2^{k-1}\left(\frac{1}{2^k}\right)$$

$$= 1 + \frac{k}{2}$$ so S_n unbounded

and $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

Decimal expansions

Let (d_n) be a sequence with $d_n \in \{0, 1, \ldots, 9\}$.

Then $\sum_{n=1}^{\infty} \frac{d_n}{10^n}$ converges to some limit r, where $0 \leqslant r \leqslant 1$,

because partial sums $S_n = \sum_{n=1}^{n} \frac{d_n}{10^n}$ are increasing and bounded above by $\sum_{n=1}^{\infty} \frac{9}{10^n} = \frac{9}{10} \cdot \frac{1}{1-\frac{1}{10}} = 1$.

We say $r = 0.d_1 d_2 \cdots$ is the decimal expansion of r.

Does every number x, $0 \leqslant x \leqslant 1$, have a decimal expansion?

Pick d_1 maximal so that $\frac{d_1}{10} \leqslant x$.

Then $d_1 \leqslant 9$ because $x < 1$ and $x - \frac{d_1}{10} < \frac{1}{10}$ because d_1 max.

Pick d_2 maximal so $\frac{d_2}{100} \leqslant x - \frac{d_1}{10}$, then $d_2 \leqslant 9$ because

$x - \frac{d_1}{10} < \frac{1}{10}$, and $x - \frac{d_1}{10} - \frac{d_2}{100} < \frac{1}{100}$ because d_2 maximal.

Inductively pick d_n such that $\frac{d_n}{10^n} \leqslant x - \sum_{j=1}^{n-1} \frac{d_j}{10^j}$ so that

$$0 \leqslant x - \sum_{j=1}^{n} \frac{d_j}{10^j} < \frac{1}{10^n}.$$

Then LHS $\to 0$, RHS $\to 0$

by Sandwich theorem, $x - \sum_{j=1}^{\infty} \frac{d_j}{10^j} = 0$ i.e. $x = 0.d_1 d_2 \cdots$

Can we have $0.a_1 a_2 \cdots = 0.b_1 b_2 \cdots$?

We may suppose $a_j = b_j$ for $j < k$ and $a_k < b_k$ for some k.

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

so must have $b_k = a_k + 1$ and $a_j = 9$, $b_j = 0$ for $j > k$.

e.g. $0.4799\cdots = 0.4800\cdots$

A decimal is <u>periodic</u> if, after a finite number of terms, say ℓ digits, it repeats in blocks of length k say i.e. there exist ℓ, k such that $d_n = d_{n+k}$ for all $n > \ell$.

A periodic decimal is rational:

e.g. $x = 0.7932\ 157\ 157\ 157\cdots$

because $10^4 x - 7932 = 0.157\ 157\cdots$

$$= 157 \sum_{j=1}^{\infty} \frac{1}{10^{3j}} = 157 \cdot \frac{1}{10^3} \cdot \frac{1}{1-\frac{1}{10^3}} = \frac{157}{10^3 - 1}$$

so $x \in \mathbb{Q}$

Conversely, if x is rational, then x has a periodic decimal expansion.

To see this, say $x = \frac{p}{2^a 5^b q}$ where $(q, 10) = 1$, $a, b \in \mathbb{Z}_0^+$ and $(p, q) = 1$.

Then $10^{\max(a,b)} x = \frac{t}{q} = n + \frac{k^c}{q}$ where $n, k^c \in \mathbb{Z}$

and $0 \leq c < q$. By Fermat–Euler, $10^{\phi(q)} \equiv 1 \pmod q$

i.e. $10^{\phi(q)} - 1 = kq$ where $k \in \mathbb{N}$, so

$$\frac{c}{q} = \frac{kc}{kq} = kc \sum_{j \geq 1} \frac{1}{10^{j\phi}} \rightsquigarrow \frac{1}{10^\phi} \cdot \frac{1}{1-\frac{1}{10^\phi}} = \frac{1}{10^\phi - 1}$$

Since $0 \leq kc < kq$ we can write kc as a ϕ-digit number $d_1 d_2 \cdots d_\phi$ then $\frac{c}{q} = 0.d_1 d_2 \cdots d_\phi d_1 d_2 \cdots d_\phi \cdots$

L20.3 Shift to right to see x periodic.

Exercise $0.0110\,1010\,0001\cdots$ (1s in prime places) is irrational

$0.2357\,11\,13\,17\,19\,23\,29\cdots$ is irrational

We define $e = \sum_{j=0}^{\infty} \frac{1}{j!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$

Note the limit exists because partial sums are increasing and bounded above by $1 + 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 3$.

Is e rational? Suppose $e = p/q$.

Since $2 < e < 3$, $q \geq 2$.

Then $q!\,e \in \mathbb{N}$. But this is

$$q! + q! + \frac{q!}{2!} + \frac{q!}{3!} + \cdots + \frac{q!}{q!} + \frac{q!}{(q+1)!} + \cdots$$

$$= N + x \text{ where } N \in \mathbb{N} \text{ and } x = \frac{q!}{(q+1)!} + \cdots$$

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

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

So $0 < x < 1$ contradicting $q!\,e \in \mathbb{N}$. So e is irrational.

An algebraic number is the root of a polynomial with integer (rational) coefficients.

Rationals are algebraic: $x = \frac{p}{q} \Rightarrow qx - p = 0$.

$\sqrt{2}$ is algebraic, root of $x^2 - 2 = 0$.

A number is <u>transcendental</u> if it is not algebraic.

Do transcendental numbers exist?

Let $L = \sum_{n \geq 1} \frac{1}{10^{n!}} = 0.11\,0001\,0\cdots\,010\cdots$ (1 in the 24^{th} place)

<u>Theorem</u> (Liouville 1851): L is transcendental

Hermite (1873) showed e transcendental.

Lindemann (1882) e^x is transcendental if x is algebraic.
So $\pi = e^i$ is ~~alge~~ transcendental since $e^{i\pi} - 1 = 0$

(hence squaring circle impossible)

Gelfond - Schneier (1934)

α^β is transcendental if α algebraic, β irrational

Baker (1968) did more

Proof (of Liouville): Suppose instead $f(L) = 0$ for some polynomial f of degree k, say, with integer coefficients.

Then $f(x) = (x - L)\, g(x)$ where

$$g(x) = b_{k-1} x^{k-1} + b_{k-2} x^{k-2} + \cdots + b_0 .$$

Let $B = |b_{k-1}| + |b_{k-2}| + \cdots + |b_0|$, so

$|g(x)| \le B$ for $0 \le x \le 1$.

Let $s = \sum_{j=1}^{m} \frac{1}{10^{j!}}$ be m^{th} partial sum, m to be chosen shortly.

Let $q = 10^{m!}$ so $s = \frac{\text{integer}}{q}$.

Pick m so that

$m > k$
$q > 2B$
$f(s) \neq 0$

} for each condition only finitely many m fail it (because f has $\le k$ roots)

Then $f(s) = \frac{\text{integer}}{q^k} \neq 0$, so $|f(s)| \ge \frac{1}{q^k}$.

But $L - s = \sum_{j=m+1}^{\infty} \frac{1}{10^{j!}} = \frac{1}{q^{m+1}} + \frac{1}{q^{(m+1)(m+2)}} + \cdots$

$$\le \frac{1}{q^{m+1}} \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right)$$

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

So $\frac{1}{q^k} \le |f(s)| = |L - s|\,|g(s)| \le \frac{2B}{q^{m+1}}$ which is false. □

§6 Countability

Recall we counted sets by constructing bijections with sets of known size, e.g. bags of fruit $\longleftrightarrow$ binary strings

Normally, we construct a bijection with some set $[n] = \{1, \dots, n\}$.

Lemma 6.1 If $f : [n] \to [n]$ is injective then it is surjective.

Proof By induction on n. True for $n = 1$. Let $n > 1$.
Let $j = f(n)$. Let $g : [n] \to [n]$ be:

$$g(j) = n, \quad g(n) = j, \quad g(i) = i \text{ if } i \neq j, n$$

Then g is a bijection. The map

$g \circ f : [n] \to [n]$ is injective and $gf(n) = n$.

So define $h : [n-1] \to [n-1]$ by $h(i) = gf(i)$. This exists and is injective. By induction hypothesis, h is surjective, so bijective. Hence so is gf. Hence so is f. □

Corollary 6.2 If A is a set and $f : A \to [n]$, $g : A \to [m]$ are bijections, then $n = m$.

Proof We may suppose $m \geq n$. Let $h : [n] \to [m]$, $h(i) = i$.
Then $[m] \xrightarrow{g^{-1}} A \xrightarrow{f} [n] \xrightarrow{h} [m]$ is injective. By Lemma 6.1, it is surjective. So h is surjective. So $n = m$. □

Definition The set A is *finite* if $A = \emptyset$ or there exists $n \in \mathbb{N}$ and a bijection $A \to [n]$.

The *size* of A, denoted by $|A|$, is n (and $|\emptyset| = 0$).

By the Corollary, $|A|$ is well-defined.

Lemma 6.3 Let $S \subset \mathbb{N}$. Then either S is finite or there exists a bijection between S and $\mathbb{N}$.

Call it $g: \mathbb{N} \to S$

Remark g is "counting" S

Proof If S is not $\emptyset$, there is, by WOP, a least element $s_1 \in S$. If $S \setminus \{s_1\} \neq \emptyset$ there is a least element s_2. If $S \setminus \{s_1, s_2\} \neq \emptyset$, then it has a least element s_3, and so on.

If at some point this process stops, then $S = \{s_1, \ldots, s_n\}$ is finite. If it goes on forever, the map $g: \mathbb{N} \to S$ given by $g(i) = s_i$ is well-defined because every i has a unique s_i, and is injective. Is it surjective? Yes, because if $k \in S$, then $k \in \mathbb{N}$ and there are $< k$ elements of S less than k, i.e. $k = s_i$ for some $i \leq k$. □

Definition The set A is countable if it is finite or there is a bijection between A and $\mathbb{N}$.

Theorem 6.4 The following are equivalent:

(i) A is countable

(ii) There is an injection $A \to \mathbb{N}$

(iii) There is a surjection $\mathbb{N} \to A$ (note A could be $\emptyset$)

Proof Plainly (i) $\Rightarrow$ (ii). Conversely if there is an injection $f: A \to \mathbb{N}$, then f gives a bijection $A \to f(A) = S$. If S is finite, so is A. If is S is infinite, there is a bijection between S and $\mathbb{N}$ and so $A \to S \to \mathbb{N}$ is a bijection. Hence (ii) $\Rightarrow$ (i).

L 21.4

Plainly (i) ⇒ (iii). Conversely, if $A \neq \emptyset$ and there is a surjection $f: \mathbb{N} \to A$, define $g: A \to \mathbb{N}$ by $g(a) = \min f^{-1}(\{a\})$, (preimage) which exists by WOP. g is an injection, so by (ii) A must be countable. □

Examples the map $f: \mathbb{Z} \to \mathbb{N}$

$$n \to \begin{cases} 2n & \text{if } n > 0 \\ 1-2n & \text{if } n \leq 0 \end{cases}$$

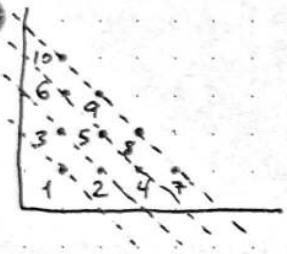
is a bijection so $\mathbb{Z}$ is countable.

This example shows that finding bijections is tedious.

$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is injective (by FTA)

$(a,b) \to 2^a 3^b$ so by Thm (ii) $\mathbb{N} \times \mathbb{N}$ is countable

In fact we can construct a bijection in this case



$$(a,b) \to \binom{a+b}{2} - a + 1$$

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

Observe: if B is countable, so $\exists$ inj. $B \to \mathbb{N}$ and if we have an injection $A \to B$, then A is countable (because $A \to B \to \mathbb{N}$ injective).

$\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ is injective

$p/q \to (p, q)$

$\therefore \mathbb{Q}$ countable

$0 \to (0, 0)$

Also $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is countable because we can inject $\mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ so inject $(\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N}$ which we know is countable.

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

Theorem: A countable union of countable sets is countable.

Proof: Let I be a countable index set and for each element $\alpha \in I$ let A_α be a countable set.

We want to show $A = \bigcup_{\alpha \in I} A_\alpha$ is countable.

I is countable so there exists an injection $f : I \to \mathbb{N}$ and $\forall \alpha$, A_α is countable, so there exists an injection $g_\alpha : A_\alpha \to \mathbb{N}$.

Construct injection $h : A \to \mathbb{N} \times \mathbb{N}$ as follows:

For each element a in $A = \bigcup_{\alpha \in I} A_\alpha$ pick $m = \min \{ j \in \mathbb{N} : a \in A_\alpha, f(\alpha) = j \}$ which exists by WOP.

Let α be such that $f(\alpha) = m$ (α unique since f injective).

Let $h(a) = (m, g_\alpha(a))$.

Then h is injective. □

Example $\mathbb{Q} = \bigcup_{n \geq 1} \frac{1}{n}\mathbb{Z} = \bigcup_{n \geq 1} \{ m/n : m \in \mathbb{Z} \}$ is countable.

Theorem The set of algebraic numbers is countable

Proof Let $\mathcal{P}_k$ be the set of polynomials of degree k with integer coefficients. The map

$$a_k z^k + a_{k-1} z^{k-1} + \cdots + a_1 z + a_0 \to (a_k, a_{k-1}, \ldots, a_0)$$

is an injection $\mathcal{P}_k \to \mathbb{Z}^{k+1}$, and, since $\mathbb{Z}^{k+1}$ is countable, so is $\mathcal{P}_k$.

Let $\mathcal{P}$ be the set of all polynomials with integer coefficients. Then $\mathcal{P} = \bigcup_{k \in \mathbb{N}} \mathcal{P}_k$ is a countable union of countable sets, so is countable. For each polynomial $P \in \mathcal{P}$, let R_P be the set of its roots. Then R_P is finite. Then the set of algebraic numbers, $\bigcup_{P \in \mathcal{P}} R_P$ is a countable union of countable sets, so is countable. ☺

L22.3

Do uncountable sets exist?

Theorem: $\mathbb{R}$ is uncountable

Proof: If $\mathbb{R}$ were countable, then we can list all the reals as

$r_1, r_2, r_3, \ldots$

Write each r_n in decimal form in some way.

$r_1 = n_1 \cdot d_{11} d_{12} d_{13} \cdots$

$r_2 = n_2 \cdot d_{21} d_{22} d_{23} \cdots$

$r_3 = n_3 \cdot d_{31} d_{32} d_{33} \cdots$

$\vdots$

Define $r = 0.d_1 d_2 d_3 \cdots$ by

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

This r has only one decimal expansion and is not in the list.
(because $\forall n,\ r \neq r_n$).

This contradicts the assumption that $\mathbb{R}$ is countable. □

This is known as "the diagonal argument" (Cantor 1870s)

Corollary: there are uncountably many transcendentals

Recall $\mathcal{P}X = \{ Y : Y \subset X \}$. Suppose $\mathcal{P}\mathbb{N}$ is countable.
So $S_1, S_2, \ldots$ are the subsets of $\mathbb{N}$.
Let $S = \{ n \in \mathbb{N} : n \notin S_n \}$. Then S is not in the list.
Hence $\mathcal{P}\mathbb{N}$ is uncountable.

(This is a diagonal argument)

Let Σ be the set of all functions $\mathbb{N} \to \mathbb{N}$ (set of "natural" sequences).

Suppose Σ were countable so we can write its elements as

$f_1, f_2, \ldots$

But then f given by $f(n) = \begin{cases} 1 & \text{if } f_n(n) \neq 1 \\ 2 & \text{otherwise} \end{cases}$

is not in the list. Hence Σ is uncountable.

Let Σ^* be the set of bijections $\mathbb{N} \to \mathbb{N}$. Then Σ^* is also uncountable. Even the subset $\Sigma^{**} \subset \not\Sigma^*$ is uncountable, where Σ^{**} is the set of bijections f where, for each n, either

(i) $f(2n-1) = 2n-1$ and $f(2n) = 2n$

or (ii) $f(2n-1) = 2n$ and $f(2n) = 2n-1$.

Each such f is encoded by a 0-1 sequence $(a_n)_{n=1}^{\infty}$ where

$a_n = 0$ if (i) holds and $a_n = 1$ if (ii) holds.

Since a 0-1 sequence is an indicator function, the set of 0-1 sequences is bijected with $\mathcal{P}\mathbb{N}$.

So we get a bijection $\mathcal{P}\mathbb{N} \leftrightarrow 2^{\mathbb{N}} \leftrightarrow \Sigma^{**}$

$\mathbb{R}$ is "more infinite" than $\mathbb{N}$

We say the two sets A, B "have the same cardinality" if there is a bijection between the two sets.

We say $\mathbb{N}$ has cardinality $\aleph_0$ (the smallest infinite cardinality)

We say $\mathbb{R}$ has cardinality $\mathfrak{c}$, the "continuum".

Theorem: let A be a set. Then there is no surjection $A \to \mathcal{P}A$.

Proof: Suppose we have $f: A \to \mathcal{P}A$ surjective.

Let $S = \{a \in A : a \notin f(a)\}$.

Since f is surjective, $\exists\ s \in A$ s.t. $f(s) = S$.

Is $s \in S$? If so, $s \notin S$ by def^n of S.

If not, then $s \in S$ by def^n of S. Contradiction.

So f does not exist. □

Hence the cardinality of $\mathcal{P}A$ is "greater" than that of A.

In particular, there are infinitely many different cardinalities.

Constructing bijections can sometimes be done.

$(0,1) \leftrightarrow \not{\mathbb{R}}\ (1,\infty)$ using $x \to \frac{1}{x}$

$(0,1) \leftrightarrow (0,\infty)$ using $x \to \frac{1}{x} - 1$

$(-1,1) \leftrightarrow \mathbb{R}$ using $\begin{cases} x \to \frac{1}{x} - 1 & \text{if } x > 0 \\ 0 \to 0 \\ x \to \frac{1}{x} + 1 & \text{if } x < 0 \end{cases}$

$(0,1) \leftrightarrow (-1,1)$ using $x \to 2x - 1$

Hence $(0,1)$ has cardinality $\mathfrak{c}$

What about $\mathcal{P}\mathbb{N}$?

Since there's a bijection between $\mathbb{N}$ and $\mathbb{Q}$ then there's a bijection $\mathcal{P}\mathbb{N}$ and $\mathcal{P}\mathbb{Q}$.

There is a map $\mathbb{R} \to \mathcal{P}\mathbb{Q}$ is an injection from $\mathbb{R}$

$r \to \{q \in \mathbb{Q} : q < r\}$

to $\mathcal{P}\mathbb{Q}$. So we conclude that there's an injection from $\mathbb{R}$ to $\mathcal{P}\mathbb{N}$.

The map $\mathcal{P}\mathbb{N} \to \mathbb{R}$

$S \to 0.\, i_S(1)\, i_S(2) \ldots$

is an injection i_S is the indicator function

Theorem: (Cantor, Bernstein, Schröder)
Suppose there are injections $A \to B$ and $B \to A$. Then there is a bijection $A \to B$.

Proof: Consider the function diagrams showing $f: A \to B$ and $g: B \to A$.
(potato arrow diagram)
Each point in the set $A \cup B$ has exactly one arrow going out of it, and at most one arrow in.

Define an equivalence relation $\sim$ on $A \cup B$ by
$u \sim v$ if there is a finite chain of arrows from u to v or from v to u. (check)

Consider an equivalence class.
There are 3 possibilities
(i) it's a one-way infinite path starting at some point w
(ii) it's a two-way infinite path
(iii) it's a finite cycle (check)

We define h on each equivalence class.

In case 1, if $w \in B$, we define $h = g^{-1}$, ~~otherwise~~

In all other cases, let $h = f$.

□

The "continuum hypothesis" asserts there is no cardinality between $\aleph_0$ and c.

Shown by Cohen to be independent from ZFC.

§ 7. Bertrand's Postulate

- Bertrand (1845-ish) postulated that there is always a prime between n and $2n$.

The primes $2, 3, \ldots, 2503$ show it to be true for $n \leq 2^{11} = 2048$.

Bertrand checked it for $n \leq 3{,}000{,}000$

Chebyser (1850) proved it.

Erdös (1932) gave very simple proof based on properties of binomial coefficients.

- 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 $\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}$.

Lemma: if p is prime and some power of p^k divides $\binom{2n}{n}$ then $p^k \leq 2n$.

Proof: let ℓ be the largest power of p with $p^\ell \leq 2n$.

- The power of p dividing $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

So $k \leq \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor$ (power of p dividing $\binom{2n}{n}$)

$$= \sum_{i=1}^{\ell} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \quad \text{since } i > \ell \text{ are zero}$$

$$\leq \sum_{i=1}^{\ell} 1 \quad \text{because } \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$$

$= \ell$, so $k \leq \ell$ and we are done. □

- **Lemma:** for all $m \in \mathbb{N}$, $\prod_{p \leq m} p \leq 4^m$, the product of all primes $\leq m$ is at most 4^m

Proof: proceed by induction on m; true for $m \leq 2$.

If $m > 2$ and m is even then

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

If $m = 2k+1$ is odd, then all primes $k+2 \leq p \leq 2k+1$ divide $\binom{2k+1}{k} = \frac{(2k+1)!}{k!(k+1)!} = \binom{2k+1}{k+1}$.

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

By the induction hypothesis,

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

□

Theorem: for all n, there exists a prime with $n < p \leq 2n$.

Proof: the prime factors of $\binom{2n}{n}$ are all $< 2n$.

If the theorem fails, they are all $\leq n$.

Crucial fact: there is no prime factor p in the range $\frac{2n}{3} < p \leq n$, for such a factor divides $(2n)!$ exactly twice and divides $n!$ exactly once.

Hence all prime factors of $\binom{2n}{n}$ are at most $\frac{2n}{3}$.

Consider the prime factorisation of $\binom{2n}{n}$. By the first lemma, each prime contributes at most $2n$ to the product.

Moreover if $p > \sqrt{2n}$ then p contributes at most p to the product. (because $p^2 > 2n$).

Using the second lemma we now have

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{p > \sqrt{2n}}^{p \leq \frac{2n}{3}} p \leq (2n)^{\sqrt{2n}} \prod_{p \leq \frac{2n}{3}} p \leq$$

$$= (2n)^{\sqrt{2n}} \, 4^{2n/3}.$$ This fails for n large.

To find a bound on how large n need be, we have

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

Clearly $(2n+1) \leq (2n)^2 \leq (2n)^{\sqrt{2n}/3}$ for $n \geq 18$

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

or $4^n \leq (2n)^{4\sqrt{2n}}$

Put $r = \sqrt{2n}$ so $r^2 = 2n$,

then $4^{r^2/2} \leq r^{8r}$

or $2^r \leq r^8$.

This fails for $r = 2^6 = 64$ and for larger r. So the proof works for $n \geq 2^{11}$, and we know it to be true for smaller n. □

Let $\pi(x)$ be the number of primes $\leq x$.

Euclid showed $\pi(x) \geq \log\log x$.

Erdős showed $\pi(x) \geq \log x$.

The Prime Number Theorem asserts $\pi(x) \sim \dfrac{x}{\log x}$.

We can get this approximately (Chebyshev)

a) the primes p dividing $\binom{2n}{n}$ are each $\leq 2n$ and there are at most $\pi(2n)$ of them. By the first lemma,

$$\binom{2n}{n} \leq (2n)^{\pi(2n)} \quad \text{and} \quad \binom{2n}{n} \geq \frac{2^{2n}}{2n+1} \geq 2^n \quad \text{so}$$

$$\pi(2n) \geq \frac{n}{\log_2 2n} \quad \text{giving} \quad \pi(x) \geq \frac{x}{2\log_2 x}$$

b) the second lemma implies $4^x \geq \prod_{\sqrt{x} < p \leq x} p > (\sqrt{x})^{\pi(x) - \pi(\sqrt{x})}$

$$\text{so} \quad \pi(x) < \frac{4x}{\log_2 x} + \pi(\sqrt{x}) < \frac{4x}{\log_2 x} + \sqrt{x} < \frac{5x}{\log_2 x}$$

for large x.