08/10/10

Numbers and Sets ①

Wesley Hamilton Davenport

$\mathbb{N} = \{1, 2, 3, \ldots\}$ set of natural numbers

$n \in \mathbb{N}$
- n is an element of $\mathbb{N}$
- n is a natural number
- n is a member of $\mathbb{N}$

thing > external jargon

eg sandwich > nothing

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

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ integers

$\mathbb{Q}$ rational numbers, fractions

$\mathbb{R}$ real numbers

$\mathbb{C}$ complex numbers

We assume standard properties

$a + b = b + a$, $ab = ba$ commutativity

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

A function $f : A \to B$ is a rule assigning to each element $a \in A$ some element $f(a) \in B$

PROOFS

A proof is a sequence of true statements without logical gaps; a logical argument establishing some conclusion.
We have to begin somewhere with agreed assumptions (axioms)

We want to prove things because:
- we want to know they are true
- we hope to gain insight into why they are true
- we might be lucky and the proof is beautiful

Examples of statements

1. Infinitely many primes of the form $n^2 + 1$
2. Always a prime between n and $2n$
3. There is no computer program that can factorise an n digit number in n^3 steps

4. For every polynomial $p(x) = a_n x^n + \dots + a_0 \quad a_i \in \mathbb{C}$
not all $a_i, \dots, a_0 = 0$
There exists $z \in \mathbb{C}$ with $p(z) = 0$
5. $m \times n = n \times m$ for all $m, n \in \mathbb{N}$
6. $2 + 2 = 4$

Statements

1. Probably true? Unproved and unsure, $p(n \text{ is prime}) \approx \frac{1}{\log n}$
For n^2+1, expect infinite. $2^{2^n}+1$, expect finite
2. True and proved
3. Unproved and unsure
4. Fundamental theorem of Algebra, ~~true~~ proved true.
5. Food for thought
6. Is proof necessary?

PROOFS and NON PROOFS

Assertion: for all $n \in \mathbb{N}$, $n^3 - n$ is a multiple of 3

Proof $n^3 - n = (n-1)n(n+1)$ Three consecutive integers
One must be divisible by 3.
Hence so is the product □

A: If n^2 is even, so is n.
P: If n is even, $n = 2k$, $n^2 = 4k^2$, even ✗

Not a proof, we showed n even $\Rightarrow n^2$ even (Though statement is true)
We wanted n^2 even $\Rightarrow n$ even

A: $n^2 \mid 9$, then $n \mid 9$ P: $n = 9k$, $n^2 = 81k^2$
Similarly False Proof and statement is actually false

Counterexample $6 \nmid 9$; $6^2 = 36 \mid 9$
One is enough

Numbers and sets (1)

Proper Proof that if n^2 is even, so is n.

Suppose on the contrary n is odd.
So $n = 2k+1$ $\quad n \in \mathbb{Z}$
But then $n^2 = 4(k^2+k)+1$, odd
contradicting assumption

1/10/16

Numbers and Sets (2)

Winstanley Lecture Theatre, Trinity 3.30

Assertion: The solution of $x^2 - 5x + 6 = 0$ is $x = 2$ or $x = 3$

actually two assertions:
i) $x = 2$, $x = 3$ are solutions
ii) No other solutions exist

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

We can write "$P \Rightarrow Q$" and "$Q \Rightarrow P$" as "$P \Leftrightarrow Q$" mean "P is equivalent to Q" "P is true if and only if Q is true" "P iff Q"

Proof i) if $x = 2$ or $x = 3$
then $x - 2 = 0$ or $x - 3 = 0$
so $(x-2)(x-3) = x^2 - 5x + 6 = 0$
ii) if $x^2 - 5x + 6 = (x-2)(x-3) = 0$
So $x - 2 = 0$ or $x - 3 = 0$
so $x = 2$ or $x = 3$

Alternatively

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

IMPORTANT! Uses iff

Assertion Every positive real number is ≥ 1

Flawed → **"Proof"** Let r be the smallest +ve real number
Either $r < 1$ or $r = 1$ or $r > 1$ (trichotomy)
If $r < 1$ then $0 < r^2 < r < 1$ a contradiction
If $r > 1$ then $0 < \sqrt{r} < r < 1$ a contradiction
So $r = 1$

FALSE! Because there is no smallest +ve real number

Moral Every claim must be justified

7 – 7

If P and Q are assertions, we can (but 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 that of P and Q.

Truth Tables.

P	Q	$P \wedge Q$
f	f	f
f	t	f
t	f	f
t	t	t

P	Q	$P \vee Q$
f	f	f
f	t	t
t	f	t
t	t	t

P	$\neg P$
f	t
t	f

P	Q	$P \Rightarrow Q$
f	f	t
f	t	t
t	f	f
t	t	t

Note e.g. $\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$
$P \Rightarrow Q$ equivalent $(\neg P) \vee Q$
Hence also to $(\neg Q) \Rightarrow (\neg P)$

Quantifiers are often used. "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 $x \in \mathbb{R}$"
$\forall x \in \mathbb{R}\ P(x)$ means P is true for all $x \in \mathbb{R}$
$\neg(\forall x \in \mathbb{R}\ P(x))$ means $\exists x \in \mathbb{R}\ \neg P(x)$
$\neg(\exists x \in \mathbb{R}\ P(x))$ means $\forall x \in \mathbb{R}\ \neg P(x)$

Order of $\forall$, $\exists$ matters. "Something is wrong with everybody."

14/10/10

Numbers and Sets (2)

Proof of Fundamental Theorem of Algebra

Assertion If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

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

then $\exists\, z \in \mathbb{C}$, $p(z) = 0$

Proof Choose $z \in \mathbb{C}$ with $|p(z)|$ smallest

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

If $|p(z)| \neq 0$, write

$p(z+h) = p(z) + b_1 h + \dots + b_n h^n$

Let $L = \min\{j : b_j \neq 0\}$

Note $b_n = a_n \neq 0$ so L is well defined

Thus $p(z+h) = p(z) + p(z) + b_L h^L + \dots + b_n h^n$

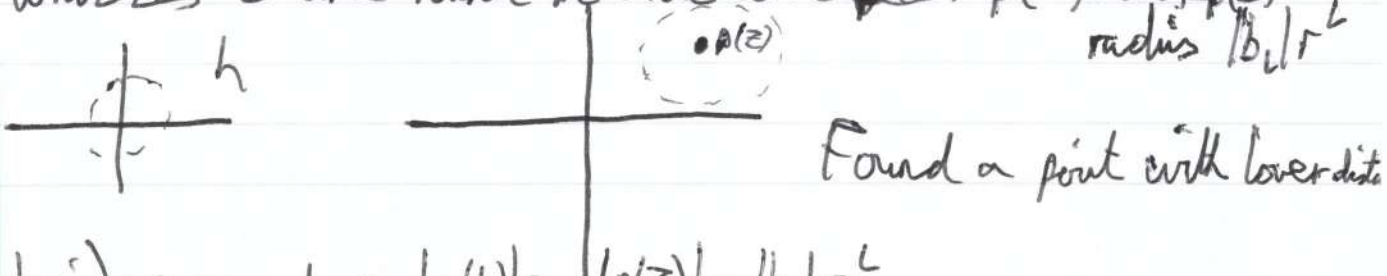
Let $q(h) = p(z) + b_L h^L$

Choose $r \in \mathbb{R}$, $r > 0$ such that

i) $|b_L| r^L < \frac{1}{2}|p(z)|$

ii) $|b_{L+1}| r + \dots + |b_n| r^{n-L} < \frac{|b_L|}{2}$

As h whizzes round the circle $|h| = r$ then $q(h)$ whizzes L times round the circle centre $p(z)$ radius $|b_L| r^L$



Found a point with lower dista

3 by i) we can choose $|q(h)| = |p(z)| - |b_L| r^L$

by ii) $|p(z+h)| \leq |q(h)| + |b_L| \frac{r^L}{2}$

$< |p(z)|$

a contradiction $\square$

- assumes there is actually a smallest value, and though closer value to zero has been found, does $p(z)$ reach zero? ← $|p(z)|$ min

We can pick $R \in \mathbb{R}$ so $|z| > R$

$|p(z)| > |p(0)| = |a_0|$

Theorem $|p(z)|$ is continuous on closed disc → includes boundary
so attains its minimum value. [Analysis I]

13/10/10

Numbers and Sets ③

Sets The order of elements in a set is immaterial and each element is counted only once.

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

Two sets are equal if they have the same elements. Equivalently
$A = B \Leftrightarrow (\forall x \; x \in A \Leftrightarrow x \in B)$
A is a subset of B, written $A \subseteq B$ or $A \subset B$, if every element of A is an element of B. Note. $A = B \Leftrightarrow A \subset B, B \subset A$

In particular, there is only one empty set $\emptyset$ with no elements.

If X is a set and P is a property of some elements of X we can write:
$\{x \in X : P(x)\}$ or $\{x \in X \mid P(x)\}$ subset of elements of X for which
Subset of X comprising the elements of X for which $P(x)$ is true
$P(x)$ is true.
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 $A \cap B = \{x : x \in A, x \in B\}$
their union is $A \cup B = \{x : x \in A \text{ or } x \in B\}$, at least one of
Clearly $(A \cap B) \cap C = A \cap (B \cap C)$
Also $A \setminus B = \{x \in A : x \notin B\}$ $\notin$ is not an element of

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 $x \in C$)
hence $x \in (A \cap B) \cup (A \cap C)$ so LHS $\subset$ RHS

if $x \in (A \cap B) \cup (A \cap C)$, ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$)
so $x \in A$ and ($x \in B$ or $x \in C$)
so $x \in A \cap (B \cup C)$
$\therefore$ LHS = RHS

If X is a set, the power set $\mathcal{P}X$ is the set of all subsets of X

$\mathcal{P}X = \{Y : Y \subset X\}$

note $\emptyset \in \mathcal{P}X \qquad X \in \mathcal{P}X$

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

$$\bigwedge_{n=1}^{\infty} A_n = A_1 \wedge A_2 \wedge \ldots = \{x : x \in A_n \text{ for all } n\}$$

More generally, if we have a collection of sets A_α, $\alpha \in I$ indexed by the set I, write

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

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

Making new sets from old by the above operations is legitimate.
This doesn't allow:

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

Russell's Paradox: For if this were a set, say Z, then $Z \in Z \Leftrightarrow Z \notin Z$
Equivalently, the collection of all sets is not a set.

A final operation is that of Cartesian Product:

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

the set of ordered pairs (a, b)
Here $(a, b) = (a', b') \Leftrightarrow a = a', b = b'$
We can extend to triple products e.g. $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$

Define $(a, b) = \{a, \{a, b\}\}$

13/10/10

Numbers and Sets ③

$f: A \to B$ a rule that assigns to each element $a \in A$ exactly one element $f(a) \in B$

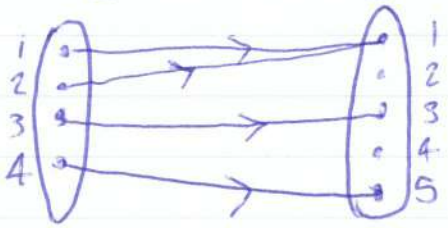
We can write $x \longmapsto f(x)$

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

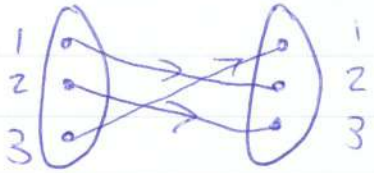
e.g. $x \longmapsto \frac{1}{3x}$ is not a function as, no $f(0)$
$x \longmapsto \pm x$ is not a function, no unique value

1. $f: \mathbb{R} \to \mathbb{R}$ $\quad x \longmapsto x^2$ NOT Inj, $f(1) = f(-1)$ NOT

2. $f: \{1, 2, 3, 4\} \to \{1, 2, 3, 4, 5\}$ Not Inj, $f(i) = f(k$



3. $f: \{1, 2, 3\} \to \{1, 2, 3\}$



INJ

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

NOT INJ

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

INJ

"Function" exactly one arrow per LH dot

Injective: $a \neq a' \Rightarrow f(a) \neq f(a')$ No two left points go to same point on right

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

Surjective: $A \to B$ is surjective if $\forall b \in B \; \exists \, a \in A \; f(a) = b$

Bijective is both

15/10/10

Numbers and Sets (4)

Injective: Exactly one element in X maps to an element in Y

$X \to Y$ Surjective: Every element in Y is mapped to by at least one in X

Bijective: Inj + Surj

$f: A \to B$ is bijection if each element in Y is mapped to exactly once

"f pairs A with B"

A permutation is a bijection $f: A \to A$

$f: A \to B$, $g: B \to C$ composition gf or $g \circ f$

the function from $A \to C$ given by $a \mapsto g(f(a))$

Note $h: C \to D$

$h \circ (g \circ f) = (h \circ g) \circ f$ associative, drop brackets

If $f: A \to B$ and $U \subset A$

We write $f(U) = \{b \in B : b = f(u) \ \exists u \in U\}$

e.g. example 4 $f(\{2,3,4\}) = \{2,3\}$

We call $f(A)$ the image of f. A is the domain of f. The range is B

Thus f is surjective if and only if $f(A) = B$

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

e.g example 4 $f^{-1}(\{2,3\}) = \{2,3,4\}$

Hence $f^{-1}(B) = A$.

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

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

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

If $a, a' \in A$ and $f(a) = f(a')$

$gf(a) = gf(a')$ i.e. $a = a'$, f is injective

If f is injective we can construct g:

If $b \in f(A)$ let $g(b) = a$ where $f(a) = b$ (only one choice as f is injective)

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

So there a map $g: B \to A$ with $fg = id_B$
We need $f(g(B)) = B$ so f must be surjective.
If f is surjective we can construct g: for each $b \in B$.
For each $b \in B$, pick some a with $f(a) = b$ and put $g(b) = a$

[The assertion that we can make all these choices is called 'the axiom of choice']

If f is a <u>bijection</u> we can find g with $fg = id_A$ and $gf = id_B$. This g is called the inverse of $f^{-1}: B \to A$
It exists if and only if f is bijective.

Relations

A relation R on a set A specifies that some elements of A are related to other elements.
We write aRb to mean "a related by R, to b"

e.g. <u>Relations on $\mathbb{N}$</u>

i) aRb if a, b have the same final digit
ii) aRb if $a \mid b$
iii) aRb if $a \neq b$
iv) aRb if $a = b = 1$
v) aRb if $|a - b| \leq 3$
vi) aRb if either $a, b \geq 5$ or $a, b \leq 4$

Formally, R is a subset of $A \times A$
We write aRb instead of $(a, b) \in R$
Notice a function $f: A \to A$ is just a special kind of relation.

15/10/10

Numbers and Sets ④

Three interesting properties of relations

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

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

transitive if $\forall a, b, c \in A$ aRb and $bRc \Rightarrow aRc$

Eg.	1	2	3	4	5	6
Reflexive	✓	✓	×	×	✓	✓
Symmetric	✓	×	✓	✓	✓	✓
Transitive	✓	✓	×	✓	×	✓

Definition A relation is an equivalence relation if it is reflexive, symmetric and transitive. So 1, 6 are equivalence relations.
The relation R on a deck of cards: "aRb if a, b have the same suit"

So is the relation ~~$\equiv$~~ on $\mathbb{R}$ which ~~is~~ is xRy if $x - y \in \mathbb{Z}$
In our examples, the relation partitions the set into related elements:
1) Partition into classes with final digit 0, 1, 2, etc
6) $\{1, 2, 3, 4\}$ $\{5, 6, 7, 8 \ldots\}$
cards clubs, spades, diamonds, hearts
$\mathbb{R}$ classes of reals with same fractional part.

Two sets are disjoint if their intersection is empty.
A partition of a set A is a collection of pairwise disjoint subsets called "pa
whose union is the whole set.

An equivalence relation is often denoted by $A \sim B$ instead of ARB
If $\sim$ is an equivalence relation, the equivalence class of $a \in A$ is
$[a] = \{ b \in A : a \sim b \}$
e.g. 1) $[97\mathbb{Z}] = \{$all numbers ending in 3$\}$
2) cards $[\heartsuit$ of clubs$] = \{$all clubs$\}$

Important observation: if we have a set A with a partition, we can define an equivalence relation such that the equivalence classes are the parts.
Define $a \sim b$ if a and b are in the same part

Theorem: Let $\sim$ be an equivalence relation on the set A. Then the equivalence classes form a partition of A.

Remark by observation, equivalence relations and partitions are 2 sides of the same coin.
Partition: Global view Equivalence relation: Local view

Since $\sim$ is reflexive we have $a \in [a]$ for all $a \in A$.
So $\bigcup_{a \in A} [a] = A$
What remains is to prove that for all elements $a, b \in A$, either the equivalence classes are disjoint, $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

Suppose $[a] \cap [b] \neq \emptyset$, say $c \in [a] \cap [b]$
So $a \sim c$ and $b \sim c$. By symmetry, $c \sim a$, so $b \sim a$ due to transitivity.
Now let d be any element of $[a]$. I.e. $a \sim d$. By transitivity $b \sim a$, $a \sim d$
$\Rightarrow b \sim d$. I.e. $d \in [b]$. Hence $[a] \subset [b]$.
Hence if $[a] \cap [b] \neq \emptyset$ then $[a] \subset [b]$, likewise $[b] \subset [a]$
Hence $[a] = [b]$. $\square$

The quotient map is the map $q: A \to$ set of equivalence classes
$q: a \longmapsto [a]$

e.g. $q:$ cards $\to$ {hearts}{spades}{clubs}{diamonds}

Division
Given $a, b \in \mathbb{Z}$, "a divides by" means
$\exists\, c \in \mathbb{Z}$ such that $b = ac$
We write $a \mid b$ to mean "a divides b" or "a is a factor of b".
$\pm 1, \pm b$ are factors of b, other factors are called proper factors.

Theorem! Division Algorithm
Given $a, b \in \mathbb{N}$, there exist numbers $q, r \in \mathbb{Z}$
with $a = qb + r$ and $0 \leq r < b$
Moreover, q and r are unique.

Proof Choose $q \in \mathbb{Z}$ maximal such that $qb \leq a$. Then $(q+1)b > a$
Thus $r = a - qb$ then $0 \leq r < b$.
Suppose $a = qb + r = q'b + r'$ where $0 \leq r, r' < b$
Then $(q - q')b = r' - r$. Now $-b < r' - r < b$
So $q - q' = 0$, $q = q'$, $r' - r = 0$, $r = r'$ □

A common factor of a and b is a number $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$.
A "highest common factor" or "greatest common divisor" of two numbers $a, b \in \mathbb{N}$ is a number $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$ and if $c \mid a$ and $c \mid b$, then $c \mid d$.

Clearly if the hcf exists it has to be the largest common factor (because every other common factor divides it) so in particular, it is unique.
We write $d = \text{hcf}(a, b) = \text{gcd}(a, b) = (a, b)$
(don't confuse with ordered pairs)
The problem is to show hcf's exist. How do we find the common factors of 4931 and 3795?
→ fundamental theorem of
Prime factorisation is a) hard b) not allowed! better ways
We spot that if $c \mid 4931$ and $3795 \Rightarrow c \mid 4931 - 3795 = 1136$
So $c \mid 3795$, $c \mid 1136$, then $c \mid 1136$, $c \mid$

20/10/10

Numbers and Sets (6)

$d = hcf(a,b)$ $\quad d|a \quad d|b$
$\forall c \quad c|a \quad c|b \Rightarrow c|d$

4931 3795

4931
−3795

factors of 4931 and 3795 are also factors of 3795 and 1136
reversible, factors of 3795 and 1136 are factors of 3795 and 4931

Conclusion
Common factors of (4931, 3795) same as (3795, 1136)

Check: if $c|a$ and $c|b$ and $u, v \in \mathbb{Z}$, then $a = kc, b = lc$ $\quad k, l \in \mathbb{Z}$
so $ua + vb = (uk + vl)c$
i.e. $c \mid (ua + vb)$, a linear combination of a and b.

Theorem Let $a, b \in \mathbb{N}$, then $hcf(a,b)$ exists.
Proof Let $S = \{ua + vb : u, v \in \mathbb{Z}\}$ be the set of all linear combinations of a and b. Let d be the smallest possible positive element of S, say, $d = xa + yb$
If $c|a$ and $c|b$ then $c|d$. We show that $d|a$ and $d|b$, then $d = hcf(a,b)$.
By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $a = qd + r$ and $0 \leq r < d$. Thus $r = a - qd = (1 - qx)a - qyb$
Linear combination of a, b, so $r \in S$. Since $0 \leq r < d$ and d is the smallest +ve element of S, $r = 0$.
Hence $d|a$, and using the same argument, $d|b$ □

respected corollary with marginally more appears

Corollary Bezout's Theorem
Let $d = hcf(a,b)$. Then $\exists x, y \in \mathbb{Z}$ $d = xa + yb$ ↑ Proof from theorem 2

Corollary Bezout's Theorem also
Let $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then there exist $u, v \in \mathbb{Z}$ with $c = ua + vb$ if and only if $hcf(a,b) \mid c$

Proof Let $d = (a, b)$. If $c = ua + vb$ then $d|c$ because $d|a$ and $d|b$
Conversely suppose $d|c$, so $c = kd$

By corollary $\exists x, y \in \mathbb{Z}$ with $d = xa + yb$ so $c = (kx)a + (ky)b$

Proofs so far are existential. How do we find d? Can we also find x, y in Bezout?

E.g. $a = 57$, $b = 42$ $\quad 57 = 1 \cdot 42 + 15$

common factors equal to hcf of 42 and 15, $\quad 42 = 2 \times 15 + 12$

15 and 12 $\quad 15 = 1 \times 12 + 3$

12 and 3 $\quad \Rightarrow (57, 42) = 3$

3 and 0, factors of 3

gives an alternative proof that hcfs exist.

Euclid's Algorithm

$a = q_1 b + r_1$

$b = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

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

$r_{n-2} = q_n r_{n-1}$ can't continue forever

Note This terminates because $b > r_1 > r_2 > \cdots \geq 0$

It works because common factors of a and b are cfs of $b, r_1, r_2, \cdots, r_{n-1}, 0$, factors of r_{n-1}; $r_{n-1} = (a, b)$

$(609953, 466007)$

$609953 = 1 \times 466007 + 143946$

$466007 = 3 \times 143946 + 34169$

$143946 = 4 \times 34169 + 7270$

$34169 = 4 \times 7270 + 5089$

$7270 = 1 \times 5089 + 2181$

$5089 = 2 \times 2181 + 727$

$2181 = 3 \times 727$

$\text{hcf}(609953, 466007) = 727$

In fact $a \geq b + r_1 > 2r_1$ so the left hand number in the algorithm halves at least every 2 steps. Hence the number of steps is at most $2 \times$ #digits in a.

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} etc $\Rightarrow$ then of a b

$57 = 2 \times 21 + 15$ $\quad \therefore (57, 21) = 3$

$21 = 1 \times 15 + 6$

$15 = 2 \times 6 + 3$

$6 = 2 \times 3 + 0$

$3 = 15 - 2 \cdot 6$

$3 = 15 - 2(21 - 15)$

$= 3 \times 15 - 2 \times 21$

$3 = 3 \times (57 - 2 \times 21) - 2 \times 21$

$3 = 3 \times 57 - 8 \times 21$

Alternate proof of Bezout and way to find x, y

20/10/10

Numbers and Sets (8)

Can we work out x, y directly?

2/10/10

Numbers and Sets (7)

Write $A_{-1} = 0$, $B_{-1} = 1$, $A_0 = 1$, $B_0 = 0$
and for $j \geq 1$ $A_j = q_j A_{j-1} + A_{j-2}$ $B_j = q_j B_{j-1} + B_{j-2}$

j	Euclid	A_j	B_j	$aB_j - bA_j$
-1		0	1	a
0		1	0	$-b$
1	$a = q_1 b + r_1$	q_1	1	$a - bq_1 = r_1$
2	$b = q_2 r_1 + r_2$	$q_2A_1 + A_0$	$q_2B_1 + B_0$	$-r_2$
3	$r_1 = q_3 r_2 + r_3$			r_3
4	$r_2 = q_4 r_3 + r_4$	$q_4A_3 + A_2$	$q_4B_3 + B_2$	$-r_4$

j^{th} line $= q_j \times (j-1)^{st}$ line $+ (j-2)^{nd}$ line

(We might prove this by induction) $\rightarrow$ Hence $aB_j - bA_j = (-1)^{j-1} r_j$

Eg. (57, 21)

	A_j	B_j
	0	1
	1	0
$57 = 2\times 21 + 15$	2	1
$21 = 1\times 15 + 6$	3	1
$15 = 2\times 6 + 3$	5	3
$6 = 2\times 3$	19	7

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

$(83, 30)$

	A_j	B_j
	1	0
$83 = 2\cdot 30 + 23$	2	1
$30 = 1\times 23 + 7$	3	1
$23 = 3\cdot 7 + 2$	11	4
$7 = 3\cdot 2 + 1$	36	13
$2 = 2\times 1$	83	30

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

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

Now $aB_n - bA_n = \pm r_n = 0$ so $\frac{a}{b} = \frac{A_n}{B_n}$

Suggests looking at the formula $A_n B_{n-1} - B_n A_{n-1}$

or more generally, $A_j B_{j-1} - B_j A_{j-1} = (q_j A_{j-1} + A_{j-2}) B_{j-1} - (q_j B_{j-1} + B_{j-2}) A_{j-1}$

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

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

In particular, the highest common factor of A_j and $B_j = 1$ $\boxed{hcf(A_j, B_j) = 1}$

How do we interpret A_3, B_3?

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

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

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

$$\frac{83}{30} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{2}}}$$

We have $\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3 + \cdots}}$ ..... a continued fraction.

Why? Let $\frac{c}{d}$ = RH fraction (c,d) to get q_1, q_2, q_3 hence, same, so same A_3, B_3 as before

Hence $\frac{A_n}{B_n} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}$

So A_3, B_3? $\frac{A_3}{B_3} = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3}}$

$\frac{A_3}{B_3}$ is the result of truncating our continued fraction for $\frac{a}{b}$.

These are called the convergents to the fraction $\frac{a}{b}$. It can be shown they approximate that fraction "very well". Many other very nice properties.

Primes

Definition $p \in \mathbb{N}$ is prime if $p > 1$ and the only factors of p are $\pm 1, \pm p$.

Every number can be written as a product of primes, for $n \in \mathbb{N}$ not itself prime, $n = ab$. If either a or b is not prime, it can be written as a product and so on, until all numbers in the product are prime.

Theorem Infinitely many primes

Proof 1 Euclid, 300BC Let $p_1, p_2 \ldots p_k$ be primes. Let N be their product $+1$. $N = p_1 p_2 \cdots p_k + 1$

Then p_1 to p_k are not factors of N, i.e $p_1 | N - p_1 \cdots p_k$ would give $p_1 | 1$.

But N is a product of primes $\Rightarrow$ larger prime than $p_1 \cdots p_k$

Or N is prime ——— $\not\Rightarrow$ □

25/10/10

Numbers and Sets (8)

There are infinitely many primes

Proof 2 Erdös 1930

Let $p_1, \ldots, p_k$ be a list of primes. Any number which is a product of these powers has the form,

$p_1^{j_1} p_2^{j_2} p_3^{j_3} \cdots p_k^{j_k} = m^2 p_1^{i_1} \cdots p_k^{i_k}$ $\quad i_k = 0$ or 1

Let $M \in \mathbb{N}$. If a number $\leq M$ is of this form, then $m < \sqrt{M}$, and there are 2^k numbers $p_1^{i_1} \cdots p_k^{i_k}$, so there are at most $\sqrt{M}\, 2^k$ numbers of this form $\leq M$.

So if $\sqrt{M}\, 2^k < M$, i.e $M > 4^k$, then some number $\leq M$ is not of this form, so has a prime factor not among $p_1, \ldots p_k$ $\square$

Note Euclid's proof shows that the k^{th} prime is at most 2^{2^k} (check by induction)
Erdös's proof shows that the k^{th} prime is $< 4^k$
In fact, it is known that the k^{th} prime $\approx k \log k$ (prime number theorem).

Can a number have more than one prime factorisation?

Clearly $21 = 3 \times 7$ is unique. But what about 295869? $(= 3 \times 7 \times 73 \times 193)$

Does $9049 \times 4009 = 6701 \times 54151$? (No)

Is $\frac{6701}{9049} = \frac{4009}{54151}$

Previous argument that every number has a factorisation does not give uniqueness because two different people might arrive at different answers. There are "arithmetical systems" (permitting addition, subtraction, multiplication where factorisation is not unique).

e.g. Even numbers $= \{2, 4, 6, \ldots\}$

"primes" in this set are $2 \times$ odd, e.g. 2, 6, 10 etc. But $60 = 2 \times 30$ and $60 = 6 \times 10$. This example has no 1 or identity but the next does.

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

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ can show these are all primes

Theorem If $a \mid bc$ and $(a,b) = 1$, then $a \mid c$.

Proof From Euclid or Bezout, there exist $u, v \in \mathbb{Z}$ with $ua + vb = 1$
$uac + vbc = c$. Then $a \mid LHS \Rightarrow a \mid c$ □

We say that a and b are coprime if the highest common factor is 1.

Corollary If p is prime and $p \mid bc$ then $p \mid b$ or $p \mid c$.

Proof $(p, b) = 1$ or p by definition of a prime. If $(p, b) = p$ then $p \mid b$.
If $(p, b) = 1$, by Theorem $p \mid c$ □

Theorem (Fundamental Theorem of Arithmetic) Every natural number is expressible as a product of primes in exactly one way. In particular, if $p_1 \cdots p_k = q_1 \cdots q_l$ where $p_1 \cdots q_l$ are all primes then $k = l$ and $p_1 \cdots p_k$ are $q_1 \cdots q_k$ in some order.

Remark We already showed there is at least one way, only uniqueness is required

Proof 1 Let $p_1 \cdots p_k = q_1 \cdots q_l$. Then $p_1 \mid q_1(q_2 \cdots q_l)$. By the corollary applied to p_1, either $p_1 \mid q_1$ or $p_1 \mid q_2 \cdots q_l$.
If $p_1 \mid q_1$, $p_1 = q_1$ because q_1 is prime, and in the second case $p_1 \mid q_2 \cdots q_l \Rightarrow p_1 \mid q_2(q_3 \cdots q_l)$. So either $p_1 = q_2$ or $p_1 \mid q_3 \cdots q_l$, and so on. Hence $p_1 = q_i$ for some i. By relabelling the qs we may assume $p_1 = q_1$. Cancelling, we obtain $p_2 \cdots p_k = q_2 \cdots q_l$. Similarly, $p_2 = q_2$ after relabelling, and so on.

Numbers and Sets (8)

Proof 2 (without Euclid etc)

Suppose FTA is false. Let $N = p_1 \cdots p_k = q_1 \cdots q_l$ be the smallest counterexample. Then no p_i = any q_j, otherwise cancelling would produce a smaller "N". So we may assume $p_1 < q_1$.

Then $N - p_1 q_2 \cdots q_l = (q_1 - p_1) q_2 \cdots q_l$ is a positive integer less than N so has a unique factorisation. One such factorisation is $(q_1 - p_1)$ plus $q_2 \cdots q_l$.

But $N - p_1 q_2 \cdots q_l = p_1 (p_2 \cdots p_k - q_2 \cdots q_l)$ so $N - p_1 q_2 \cdots q_l$ has a factorisation with p_1.

Therefore $p_1 | q_1 - p_1 \Rightarrow p_1 | q_1 \Rightarrow p_1 = q_1$ #

□

7/10/10

Numbers and Sets (9)

Remark if $a = p_1^{i_1} p_2^{i_2} p_3^{i_3} \cdots p_r^{i_r}$
$b = p_1^{j_1} p_2^{j_2} p_3^{j_3} \cdots p_r^{j_r}$
where $p_1 \cdots p_r$ are distinct primes, and i, j allowed to be 0

$$hcf(a,b) = p_1^{\min(i_1,j_1)} p_2^{\min(i_2,j_2)} \cdots p_r^{\min(i_r,j_r)}$$

Least common multiple $lcm(a,b)$, smallest integer divisible by both a and b

$$lcm = p_1^{\max(i_1,j_1)} p_2^{\max(i_2,j_2)} \cdots p_r^{\max(i_r,j_r)}$$

Moreover, any number divisible by both a and b is divisible by their lowest common multiple.

$$hcf(a,b)\, lcm(a,b) = ab$$

Counting and Integers

Pigeonhole principle. Given $(n-1)n + 1$ pigeons in n pigeonholes, some pigeonhole contains at least m pigeons.

Let X be a set. For $A \subset X$ the indicator function of A is the function $i_A : X \to \{0,1\}$, $i_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A \end{cases}$
sometimes called characteristic function χ_A
Notice $i_A = i_B \iff A = B$
Can be used to prove set identities.

$i_{A \cap B} = i_A i_B$ (i.e. $\forall x \; i_{A\cap B}(x) = i_A(x) i_B(x)$),
$i_{\bar{A}} = 1 - i_A$ [$\bar{A} = X \setminus A$ and $1(x) = 1 \; \forall x$ ie. $1 = i_X$,

We have $\overline{A \cup B} = \bar{A} \cap \bar{B}$

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

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

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

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

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

$i_A^{\,2} = i_A$ (Note $i_{A\Delta B}$ has the same parity as $i_A + i_B$)

$i_{A\Delta B} \equiv (i_A + i_B) \bmod 2$

Indicator functions are handy for finding the sizes of finite sets.

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

E.g. $$\sum_{x\in X} i_{A\cup B}(x) = \sum_x i_A(x) + \sum_x i_B(x) - \sum_x i_{A\cap B}(x)$$

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

How does it generalise?

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

$$|\bar{A}\cap\bar{B}\cap\bar{C}| = |X| - |A| - |B| - |C| + |A\cap B| + |B\cap C| + |C\cap A| - |A\cap B\cap C|$$

Principle of Inclusion-Exclusion.

Let $A_1, A_2 \ldots A_n$ be subsets of a finite set X. Then

$$|\bar{A}_1\cap\bar{A}_2\cap\ldots\cap\bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i\cap A_j| - \sum_{i<j<k} |A_i\cap A_j\cap A_k| + \ldots + (-1)^n |A_1\cap A_2\cap\ldots|$$

Equivalently

$$|A_1\cup A_2\cup A_3\cup\ldots\cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i\cap A_j| + \ldots + (-1)^{n-1} |A_1\cap A_2\cap A_3\cap\ldots\cap A_n|$$

27/10/10

Numbers and Sets (9)

Proof $i_{\bar{A}_1 \wedge \bar{A}_2 \wedge \bar{A}_3 \wedge \ldots \wedge \bar{A}_n} = i_{\bar{A}_1} i_{\bar{A}_2} i_{\bar{A}_3} \ldots i_{\bar{A}_n}$

$= (1 - i_{A_1})(1 - i_{A_2}) \ldots (1 - i_{A_n})$

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

$= 1 - \sum_i i_{A_i} + \sum_{i<j} i_{A_i \wedge A_j} - \ldots + (-1)^n i_{A_1 \wedge A_2 \wedge A_3 \wedge \ldots \wedge A_n}$

Take each indicator and sum its values over the whole set X.

$|\bar{A}_1 \wedge \bar{A}_2 \wedge \ldots \wedge \bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \wedge A_j| - \ldots$
$\ldots (-1)^n |A_1 \wedge A_2 \wedge \ldots \wedge A_n|$

Example: How many numbers ≤ 200 are coprime to 110?

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

9/10/10

Numbers and Sets (10)

Example of Inclusion-Exclusion

How many numbers ≤ 200 are coprime to 110?

Let $X = \{1, 2, \ldots, 200\}$

$A_1 = \{x : 2 | x\}$, $A_2 = \{x : 5 | x\}$, $A_3 = \{x : 11 | x\}$

$|A_1| = \lfloor \frac{200}{2} \rfloor = 100$ ← round down

$|A_2| = \lfloor \frac{200}{5} \rfloor = 40$

$|A_3| = \lfloor \frac{200}{11} \rfloor = 18$

$|A_1 \cap A_3| = \lfloor \frac{200}{22} \rfloor = 9$

$|A_1 \cap A_2| = \lfloor \frac{200}{10} \rfloor = 20$

$|A_2 \cap A_3| = \lfloor \frac{200}{55} \rfloor = 3$

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

$$\text{Answer} = |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = 200 - 100 - 40 - 18 + 20 + 9 + 3 - 1 = 73$$

How many subsets of $\{1, 2, \ldots, n\}$ are there?
There are 2^n ways to choose a subset.

Equivalently, there are 2^n indicator functions $\{1, 2, \ldots, n\} \Rightarrow \{0, 1\}$

← n choose r

Definition There are $\binom{n}{r}$ subsets of $\{1, 2, \ldots, n\}$ of size r.

So by definition $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$

More generally, the Binomial Theorem, for $n \in \mathbb{N}$

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

Proof $(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ factors}}$

When we expand the product, we get the sum of all possible products of one term (a or b) from each bracket.

The term $a^{n-r}b^r$ comes when we take 'b' from r brackets and 'a' from the remaining $n-r$ brackets: there are $\binom{n}{r}$ ways to make this choice.

$\binom{n}{r}$ is sometimes called a binomial coefficient due to this theorem.

Some identities:

$\binom{n}{r} = \binom{n}{n-r}$ choosing 'r' items to keep is the same as discarding $n-r$

$\underbrace{\binom{n}{r-1} + \binom{n}{r}}_{} = \binom{n+1}{r}$ **Pascal's Identity**

Choosing a team of r from $n+1$ players, one of whom is Rooney. LHS is teams with Rooney, and teams without.

$\binom{n}{0} = \binom{n}{n} = 1$ we can construct Pascal's Triangle.

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$$

E.g. Choose a squad of k players to send to Australia, from n players. Then choose a team of r players from the squad.

RHS: Choose the team first, then the $k-r$ other squad players from $n-r$.

$$\binom{a}{r}\binom{b}{0} + \binom{a}{r-1}\binom{b}{1} + \binom{a}{r-2}\binom{b}{2} + \cdots + \binom{a}{0}\binom{b}{r} = \binom{a+b}{r}$$

Vandermonde's Convolution

RHS: Choose r from $(a+b)$ men and women

LHS: Could choose all men, or $(r-1)$ men, 1 women, etc

29/10/10

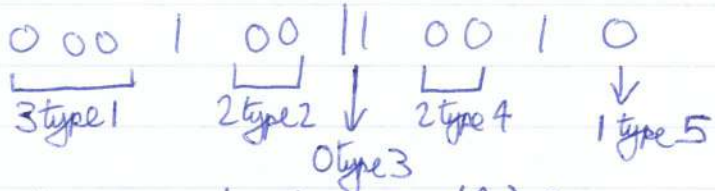
Numbers and Sets (10)

A greengrocer stocks n kinds of fruit. In how many ways can we choose a bag of r fruits?
If we are allowed only one of each, answer $= \binom{n}{r}$

But if $r=4$, allowed 2 apples, 1 pear, 1 quince...

Answer is actually $\binom{n+r-1}{r}$

Because there is a bijection from all the bags of fruit to the set of 0-1 strings $n+r-1$ with r 0s and $(n-1)$ 1s.



$n=5, r=8$

What is the numerical value of $\binom{n}{r}$?
There are $n(n-1)(n-2)\dots(n-r+1)$ to choose r elements in order.
Each subset gets chosen $r!$ times.
So it follows that $n(n-1)\dots(n-r+1) = r!\binom{n}{r}$

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

"x to the r falling"

We might write $x^{\underline{r}}$ for the polynomial $x(x-1)(x-2)\dots(x-r+1)$

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!}$$

Multiply Vandermonde's Convolution by $r!$: "falling binomial theorem"

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

A bank prepares a letter for each of its n customers to tell them how much it cares for them (at a cost of £50 per letter). There are $n!$ ways to put the n letters in the n envelopes. How many of these ways are called <u>derangements</u> where every gets a wrong letter?

Let X be the set of all ways to put into envelopes, $|X| = n!$
For each person i, let A_i ~~be~~ assignments where i gets the right letter

Want $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \dots \cap \bar{A}_n|$

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

So the answer $|\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_n| = |X| - \sum |A_i| + \sum |A_i \cap A_j| -$
$= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \dots + (-1)^n \binom{n}{n}(0)!$
$= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \dots + \frac{(-1)^n}{n!}\right] \approx \frac{n!}{e}$ for large n.

31/11/10

Numbers and Sets (11)

Well ordering and Induction

Several times we used "the largest/smallest integer such that" e.g. division algorithm, proof ∃ hcf s or had a sequence of operations "and" "and so on" eg Euclid, the A_j and B_js, every number is a product of primes, FTA, incl/excl, binomial.

We rely on the following:

(Weak) Principle of Induction

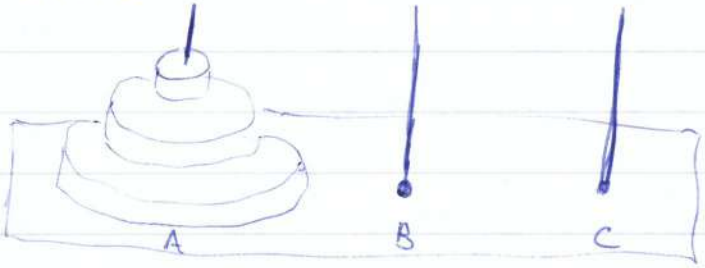
Let $p(n)$ be a statement about the number $n \in \mathbb{N}$

Suppose i) $p(1)$ is true

ii) $\forall n \in \mathbb{N}$, if $p(n)$ is true, then $p(n+1)$ is true

Then $p(n)$ is true for all n.

examples Tower of Hanoi



n rings on peg A,
Must move them to peg B.
Rules: One ring at a time, never put larger on small.

Claim: We need exactly $2^n - 1$ moves.

Proof: Let $p(n)$ be the statement, "n rings requires $2^n - 1$ moves exactly"

$p(1)$ is true.

Suppose we have $n+1$ rings.

We could move the top n rings to C, then the largest ring from A to B, then the n rings to B. Moves $\leq (2^n - 1) + 1 + 2^n = 2 \times 2^n - 1 = 2^{n+1} - 1$

Assuming $p(n)$ is true, at most $2^{n+1} - 1$ moves are needed.

At some point, the bottom ring must leave peg A, by $p(n)$ there must be at least $2^n - 1$ moves before this. At some point the bottom ring reaches B, then it takes at least $2^n - 1$ moves to get the other rings on top. by $p(n)$.

Moves $\geq 2^{n+1} - 1$ by $p(n)$

$p(n+1)$ is implied by $p(n)$. Thus by the principle of induction, $p(n)$ is true for all $n \in \mathbb{N}$ □

"Proof" **Claim** All numbers are equal.

Let $p(n)$ be "if $\{a_1, a_2 \ldots, a_n\}$ is a set of numbers, $a_1 = a_2 = a_3 = \ldots = a_n$".

$p(1)$ is true.

Suppose we have $\{a_1, a_2, \ldots, a_{n+1}\}$. Assuming $p(n)$; apply to $\{a_1, \ldots, a_n\}$ then $a_1 = a_2 = \ldots = a_n$

apply to $\{a_2, \ldots, a_{n+1}\}$ then $a_2 = a_3 = \ldots = a_{n+1}$

$p(n) \Rightarrow p(n+1)$. So principle of mathematical induction, $p(n)$ is true for all $n \in \mathbb{N}$

NOTE!! "$p(1) \Rightarrow p(2)$" fails.

Moral Check the general argument on small cases. If it doesn't work, establish these cases individually.

Claim: Inclusion-Exclusion Formula is correct.

Proof: Let $p(n)$ be the statement

"$|A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n| = \sum |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots$

$p(1)$ is true. $p(2)$ true by base' hands.

Let $n \geq 2$. Let $B_i = A_i \cap A_{n+1}$ $\quad 1 \leq i \leq n$

Then $B_i \cap B_j = A_i \cap A_j \cap A_{n+1}$

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

Now $|A_1 \cup A_2 \cup \ldots \cup A_{n+1}| = |(A_1 \cup \ldots \cup A_n) \cup A_{n+1}|$

$= |A_1 \cup A_2 \cup \ldots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n) \cap A_{n+1}|$

by $p(2)$.

$= |A_1 \cup \ldots \cup A_n| + |A_{n+1}| - |B_1 \cup \ldots \cup B_n|$

Apply $p(n)$ to both the A_i and B_i.

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

$$+ |A_{n+1}| - \sum_{i \leq n} |B_i| + \sum_{i<j \leq n} |B_i \cap B_j| - \ldots$$

$$= \sum_{i\in n} |A_i| - \sum_{i<j\in n} |A_i \cap A_j| + \sum_{i<j<k\in n} |A_i \cap A_j \cap A_k| - \dots$$

$$+ |A_{n+1}| - \sum_{i\in n} |A_i \cap A_{n+1}| + \dots -$$

Thus $p(n) \Rightarrow p(n+1)$. So by WPI, $p(n)$ is true for all n □.

WPI isn't tailored for some proofs.

Strong principle of induction

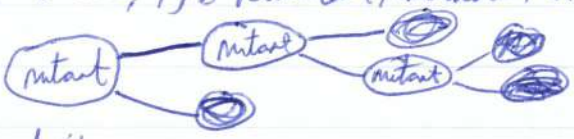
Let $p(n)$ be a statement about $n \in \mathbb{N}$.

Suppose i) $p(1)$ is true

ii) $\forall n \in \mathbb{N}$, if $p(k)$ is true $\forall k < n$ then $p(n)$ is true. (for clarity)

Then $p(n)$ is true for all $n \in \mathbb{N}$. (Note, i) is redundant, included in ii))

Example Evolutionary Trees



$p(n)$: "$n-1$ mutants yield n animals".

Proof Given a tree with n animals, remove the top mutant to get two smaller evolutionary trees with n_1 and n_2 animals. $n_1 + n_2 = n$.

Thus if $p(k)$ true for all $k < n$ then $p(n_1)$ and $p(n_2)$ are true.

So total mutants is $(n_1 - 1) + (n_2 - 2) + 1 = n - 1$.

So by SPI, $p(n)$ true for all $n \in \mathbb{N}$. □

(note, n_1, n_2 depend on the tree. did we prove $p(1)$?)

03/11/10

Numbers and Sets (12)

WPI i) $P(1)$
ii) $\forall n \quad P(n) \Rightarrow P(n+1)$
} $P(n)$ true for all n

SPI i) $P(1)$
ii) $\forall n \ (\forall k < n \quad P(k)$ is true$) \Rightarrow P(n)$
}

Theorem WPI is equivalent to SPI

Proof Clearly SPI $\Rightarrow$ WPI [Either: note $[P(n) \Rightarrow P(n+1)] \Rightarrow [P(1) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)]$
Or, any proof of something using the weak principle can be proved ~~using~~ the strong principle.

To show WPI $\Rightarrow$ SPI, assume $P(1)$ is true and $\forall n \ P(1) \wedge \ldots \wedge P(n-1) \Rightarrow P(n)$. We wish to show $P(n)$ true for all n. Let $Q(n)$ be "$P(k)$ is true for all $k \leq n$". $Q(1)$ is true. Suppose $Q(n)$ is true. Then $P(1) \wedge P(2) \wedge \ldots \wedge P(n)$ is true. Hence $P(n+1)$ is true.
Now $P(1) \wedge \ldots \wedge P(n+1)$ is true so $Q(n+1)$ is true. Thus $Q(n) \Rightarrow Q(n+1)$.
So by ~~the weak~~ WPI applied to Q, $Q(n)$ true for all n, then $P(n)$ is true for all n. □

A <u>partial order</u> on a set is a relation that is reflexive, antisymmetric and transitive.
antisymmetric: $aRb, bRa \Rightarrow b = a$

e.g. $\mathbb{N}$ is partially ordered by $|$

An order is <u>well founded</u> if every non empty subset has a minimal element (i.e. if $m \in S$ and $x < m \Rightarrow x \notin S$)

If $\forall a, b$ either $a \leq b$, $b \leq a$ the order is called a <u>total order</u>
A well founded total order is called a <u>well order</u>.

<u>Note</u> $\mathbb{Q}$ is totally ordered but not well ordered. e.g. $S = \{q \in \mathbb{Q} : q > 0\}$

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

Theorem: SPI is equivalent to WOP

Proof: To prove WOP $\Rightarrow$ SPI:
Suppose $p(1)$ true, and $(p(k)\ \forall k<n) \Rightarrow p(n)$
Suppose, contrary to SPI, $p(n)$ is not true for all n.
Let $C = \{n \in \mathbb{N}, p(n) \text{ is false}\}$
"The set of counterexamples". Then $C \neq \emptyset$ so by WOP, C has a minimal element $n \in C$. "a minimal counterexample". Now for all $k < n$, $k \notin C$ so $p(k)$ is true for $k<n$. However $(p(k)\ \forall k<n) \Rightarrow p(n)$ contradicting that $n \in C$. This contradiction implies SPI true.

To show SPI $\Rightarrow$ WOP: Let $S \subseteq \mathbb{N}$ and suppose S has no smallest element. We shall show $S = \emptyset$. Let $p(n)$ be "$n \notin S$".
Certainly $1 \notin S$ (because 1 is the smallest natural number).
$p(1)$ is true.
Suppose $p(k)$ is true $\forall k<n$. Then $k \notin S\ \forall k<n$. Thus $n \notin S$ as n would become a minimal element in S. Hence $p(n)$ true.
By SPI, $p(n)$ is true $\forall n \in \mathbb{N}$ i.e. $S = \emptyset$

WOP allows us to prove a statement P always true as follows:
If P is false, there is a <u>minimal counterexample</u>, then argue for a contradiction.

Eg. FTA, evolutionary trees

03/11/10

Numbers and Sets (12)

E.g. Can you draw a diagram with one pencil stroke returning to starting position?

Claim If and only if diagram is "connected" (can reach any point from any other) and every junction has an even number of lines.

Proof "Only if" is clear.

"If" Suppose not. Take a minimal counterexample (minimal number of lines) Start anywhere: Wander randomly until you get stuck. By evenness, you must be back at the start. The bits not covered form a collection of connected pieces each of which has the evenness property. By minimality of counterexample, each of these pieces can be drawn. So: go round your previous random tour, taking time out to traverse each uncovered piece when encountered (which will happen, as the whole thing is connected) □

"All numbers are interesting" Certainly 1 is interesting.

Proof If not, by WOP, there is a minimal counterexample.

"The smallest uninteresting number". What could be more interesting?

Hence no counterexamples □

05/11/10

Numbers and Sets (13)

WIP $\Leftrightarrow$ SIP $\Leftrightarrow$ WOP

Idea of "minimal counterexample" works with other orders.

Eg 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 $m, n > 0$

But is it well defined?

The <u>lexicographic</u> or <u>dictionary</u> order on $\mathbb{N}_0 \times \mathbb{N}_0$ is $(u,v) \leq (x,y)$ if $u < x$ or $u = x$ and $v \leq y$

The definition of $a(m,n) = a(x,y)$ where $(x,y) < (m,n)$

Definition is sound provided the order is well founded.

Note an order is well founded if and only if there is no infinite descending chain [if there is such a chain $x_1 > x_2 > x_3 > \dots$ then the set has no minimal element. Conversely if S is a set with no min element we can construct an infinite descending chain]

$\mathbb{N}_0 \times \mathbb{N}_0$ lex order is well founded, for suppose

$(u_1, v_1) > (u_2, v_2) > (u_3, v_3) > \dots$

$u_1 \geq u_2 \geq u_3 \geq \dots$ by WOP for $\mathbb{N}$, must be a minimal element, there exists k such that $u_k = u_{k+1} = u_{k+2} = \dots$

Then $v_k > v_{k+1} > v_{k+2} > \dots$ contradicting WOP for $\mathbb{N}$ $\square$

~~What is $a(4,4) = a[3, a(4,3)]$~~

~~$a(4,3) = a$~~

Peano Arithmetic

(1892) Peano defined $\mathbb{N}$ as a set with a special element 1 and a map $\mathbb{N} \to \mathbb{N}$, $n \mapsto n^+$ successor, such that:

i) $\forall n$, $n^+ \neq 1$

ii) $\forall n, m$, $n \neq m \Rightarrow n^+ \neq m^+$ (injective)

iii) That's all i.e. $A \subseteq \mathbb{N}$, $1 \in A$ and $n \in A \Rightarrow n^+ \in A$, then $A = \mathbb{N}$

Note iii) equivalent to WPI

Work to recover the usual properties of $\mathbb{N}$.

Crucial: if $n \neq 1$, $\exists m$, $n = m^+$ (follows from iii)

Now write 2 for 1^+, 3 for 2^+

Define addition by induction: $(k+1) = k^+$, $k+n = (k+m)^+$, $n = m^+$

multiplication, order on $\mathbb{N}$.

Modular Arithmetic

Definition If $a, b \in \mathbb{Z}$ have the same remainder after division by m, we say a and b are <u>congruent modulo m</u>: that is $a \equiv b \pmod m$ means $m \mid a-b$.

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

By definition, if $d \mid m$ then $a \equiv b \pmod m \Rightarrow a \equiv b \pmod d$

$21 \equiv 11 \pmod{10} \Rightarrow 21 \equiv 11 \pmod 5$

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. $\mathbb{Z}_3 = \{[0], [1], [2]\} = \{\{\ldots -3, 0, 3 \ldots\}, \{\ldots -2, 1, 4 \ldots\}, \{\ldots -1, 2, 5 \ldots\}\}$

<u>Note</u> If $a \equiv b \pmod m$ and $u \equiv v \pmod m$

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

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

$a \equiv b \pmod m$ $\quad \Rightarrow \quad a+u \equiv b+v \pmod m$

$u \equiv v \pmod m$ $\quad \Rightarrow \quad au \equiv bv \pmod m$

25/11/10

Numbers and Sets (13)

Hence we can do arithmetic modulo m. (Formally we are doing arithmetic with congruence classes).

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

Proof If so, then $2a^2\equiv 1 \pmod 3$ $\pmod 3$

But $2\cdot 0^2\equiv 0$, $2\cdot 1^2\equiv 2$, $2\cdot 2^2\equiv 2$, so no a satisfies equation

Note that all primes are either 2, or $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$

Example There are infinitely many primes with $p\equiv -1 \bmod 4$.

Proof Let $p_1,\dots,p_k$ be a list of primes $\equiv -1 \pmod 4$. Let $N=4p_1p_2\cdots p_k-1$

Then $N\equiv -1 \pmod 4$.

Now N is a product of primes $N=q_1q_2\cdots q_l$

Clearly, for all i, $q_i\neq 2$ and $q_i=$ no p_j as no $p_j\mid N$.

If all $q_j\equiv 1 \pmod 4$ then $N\equiv 1 \pmod 4$ which is false. Hence, some $q_j\equiv -1 \pmod 4$ i.e. there is a prime $\equiv -1 \pmod 4$ not in our list.

How does this proof fail if we want infinitely many primes $\equiv 1 \pmod 4$?

Example Solve $7x\equiv 2 \pmod{10}$ → We "divided by 7"

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

$3\cdot 7\cdot x\equiv 3\cdot 2 \pmod{10}$

$x\equiv 6 \pmod{10}$

28/11/10

Numbers and Sets (14)

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

(x3) $7 \times 3 \equiv 1 \pmod{10}$

$2 \mid x \equiv 6 \pmod{10}$ $\qquad x \equiv 6 \pmod{10}$

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

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

Proof Suppose u is a unit and let $d = (u, n)$
Since $n \mid uv - 1$ and $d \mid n$ so $d \mid uv - 1$
But $d \mid u$ so $d \mid 1 \Rightarrow d = 1$.

Suppose conversely that $(u, n) = 1$. Then $\exists\, v, w \in \mathbb{Z}$ such that
$uv + nw = 1. \Rightarrow uv \equiv 1 \pmod{n}$.

Important not only does v exist but we can find it efficiently by Euclid's Algorithm.

Corollary If $(a, n) = 1$ then the congruence $ax \equiv b \pmod{n}$ has a unique solution.

Proof There exists u with $au \equiv 1 \pmod{n}$ so $uax \equiv bu \pmod{n}$
$\Rightarrow x \equiv bu \pmod{n}$

What if $ax \equiv b \pmod{n}$ and $(a, n) > 1$?
Let $(a, n) = d$. Then $n \mid ax - b$ so $d \mid ax - b$ and $d \mid a$.
Hence if there is some x satisfying $ax \equiv b \pmod{n}$ then it is necessary that $d \mid b$.
If $d \mid b$, write $n = dn'$, $a = da'$, $b = db'$
Then $ax \equiv b \pmod{n} \iff ax - b = kn$ for some $k \in \mathbb{Z}$
$\iff a'x - b' = kn' \iff a'x \equiv b' \pmod{n'}$ $\qquad (a', n') = 1$

If $(a, n) = d > 1$ the congruence $ax \equiv b \pmod{n}$ is insoluble unless $d \mid b$, then the solutions are of $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

Multiple moduli

Observe $x \equiv 5 \pmod{12} \Rightarrow \begin{cases} x \equiv 5 \pmod 3 \text{ or } x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 4 \text{ or } x \equiv 1 \pmod 4 \end{cases}$

Is the converse true?

I.e. does $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4 \Rightarrow x \equiv 5 \pmod{12}$

Inspection shows yes.

Theorem (Chinese Remainder Theorem)

Let $(m, n) = 1$, and $a, b \in \mathbb{Z}$. Then there is a solution to the simultaneous congruences $x \equiv a \pmod m$ and $x \equiv b \pmod n$. Moreover, if $y \equiv x \pmod{mn}$ then y is also a solution, and there are no other solutions.

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

$vn \equiv 1 \pmod m$ so $x \equiv a \pmod m$.

Likewise $x \equiv b \pmod n$.

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 $n \mid y - x$

$\Leftrightarrow$ $mn \mid y - x$ by FTA or lcms using $(m, n) = 1$

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

Sun Zi (2c - 8c)

1) Can be extended to multiple moduli (more than two) by repetition or induct
2) It shows a congruence $\pmod{mn}$ is equivalent to one mod m and one mod n
3) We have a bijection $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$

$x \equiv a \pmod m$, $x \equiv b \pmod n \Leftrightarrow x \equiv c \pmod{mn}$

Note c is a unit $\pmod{mn}$ iff a is a unit $\pmod m$ and b is a unit $\pmod n$

08/11/10

Numbers and Sets (14)

For if $cu \equiv 1 \pmod{mn}$ then $a \equiv c \pmod{m}$ so $au \equiv cu \equiv 1 \pmod{m}$, so a is unit mod m. $cu = kmn + 1$

Conversely if c is not a unit then $(c, mn) > 1$ so $\exists$ prime p, $p \mid c$, $p \mid mn$. Then say $p \mid m$, so $p \mid a = c + km$ so $(a, m) > 1 \Rightarrow a$ is not a unit (mod m).

Definition (Euler's Totient Function)
We denote by $\phi(m)$ the number of integers a, $0 \le a \le m$ such that $(a, m) = 1$.
So $\phi(1) = 1$. Note, p is prime $\phi(p) = p - 1$

It follows from the above that $\phi(m)$ is multiplicative:
$\phi(mn) = \phi(m)\,\phi(n)$ if $(m, n) = 1$.
More generally $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$
Thus if $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ distinct primes then

$$\begin{aligned}\phi(m) &= \phi(p_1^{k_1})\,\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) \\ &= p_1^{k_1}\left(1 - \tfrac{1}{p_1}\right) p_2^{k_2}\left(1 - \tfrac{1}{p_2}\right) \cdots p_r^{k_r}\left(1 - \tfrac{1}{p_r}\right) \\ \phi(m) &= m \prod_{p \mid m}\left(1 - \tfrac{1}{p}\right)\end{aligned}$$

An alternative proof of this formula (which thus implies multiplicativity) is by inclusion exclusion.

Let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Let $X = \{0, \ldots, n-1\}$
Let $A_i = \{x \in X : p_i \mid x\}$
Then $|X| = m$, $|A_i| = \frac{m}{p_i}$
and e.g. $|A_i \cap A_j \cap A_k| = \frac{m}{p_i p_j p_k}$
Thus

$$\begin{aligned}\phi(m) = |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_r| &= m - \sum_i \frac{m}{p_i} + \sum_{i<j} \frac{m}{p_i p_j} - \sum \cdots \\ &= m\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_r}\right)\end{aligned}$$

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

$$p^k - \frac{p(1-p^k)}{1-p}$$

$$= \frac{p^k(1-p) - p(1-p^k)}{1-p}$$

$$= \frac{p^k - p^{k+1} - p + p^{k+1}}{1-p}$$

$$= \frac{p(p^{k-1} - 1)}{1-p}$$

5/11/10

Numbers and Sets (15)

Note: if a, b are units mod m then so is ab; for if $au \equiv 1$, $bv \equiv 1$ then $(au)(bv) \equiv 1$.
Thus the units (mod m) form a <u>multiplicative group</u>.
Let p be a prime. $1, 2, 3, \ldots, p-1$ are all units. The units come in pairs a, b which are inverses to each other, plus some elements which are self inverse, i.e. $x^2 \equiv 1 \pmod p$. Now:

$$x^2 \equiv 1 \pmod p \iff p \mid x^2 - 1 = (x+1)(x-1)$$
$$\iff p \mid x-1 \text{ or } p \mid x+1 \iff x \equiv 1 \text{ or } x \equiv -1 \pmod p$$

Thus 1 and -1 are both self inverse: others come in inverse pairs:
1 and 10 are self inverse, (2, 6), (3, 4), (7, 8), (5, 9) are pairs.

<u>Theorem</u> (Wilson's Theorem) $(p-1)! \equiv -1 \pmod p$ if p is prime.

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

<u>Theorem</u> (Fermat's Little Theorem) Let p be prime.
Then $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$.
Or $a^{p-1} \equiv 1 \pmod p$, $a \not\equiv 0 \pmod p$

<u>Remark</u> 2nd statement implies the first, but conversely, the first implies the second, because if $a \not\equiv 0$, a is a unit and we obtain the second statement (Cauchy)

<u>Proof 1</u> The numbers $\{1, \ldots, p-1\}$ are units so they form a group. So $a^{p-1} \equiv 1$

<u>Proof 2</u> If $a \not\equiv 0$ then a is a unit. Thus $ax \equiv ay$ iff $x \equiv y$.
Hence $a1, a2, a3, \ldots, a(p-1)$ are pairwise incongruent (mod p). So they are congruent to $1, 2, \ldots, p-1$ in some order.
Hence $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$
$a^{p-1}(p-1)! \equiv (p-1)!$ $(p-1)!$ is a product of units, it is a unit
Thus $a^{p-1} \equiv 1 \pmod p$. □

Proof 3 If $0<k<p$ then $\binom{p}{k} \equiv 0 \pmod p$

So if $a, b \in \mathbb{Z}$ then

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p} b^p$$
$$\equiv a^p + b^p \pmod p$$

Now $0^p \equiv 0$, $1^p = 1$, $2^p \equiv (1+1)^p \equiv 1^p + 1^p \equiv 2$

$3^p \equiv (2+1)^p \equiv 2^p + 1^p \equiv 2+1 \equiv 3$, proceed by induction $\square$

Both Wilson and Fermat fail if the modulus is not prime. But Fermat does generalise.

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

Proof Let $U = \{x \in \mathbb{N} : 0<x<m, (x,m)=1\}$ $\quad |U| = \phi(m)$
be the $\phi(m)$ numbers $<m$ coprime to m.
Since a is a unit $ax \equiv ay \Leftrightarrow x \equiv y$
So if $U = \{u_1, u_2, \ldots, u_{\phi(m)}\}$ then $au_1, au_2, \ldots, au_{\phi(m)}$ are distinct units $\pmod m$ so are congruent to $u_1, u_2, \ldots, u_{\phi(m)}$ in some order. Hence

$$au_1 \cdot au_2 \cdots au_{\phi(m)} \equiv u_1 u_2 \cdots u_{\phi(m)}$$
$$a^{\phi(m)} Z \equiv Z \quad \text{where } Z = u_1 u_2 \cdots u_{\phi(m)}$$

Thus $a^{\phi(m)} \equiv 1 \pmod m$ $\square$

e.g. $p=5$

Squares $1^2, 2^2, \ldots, (p-1)^2$ are squares $\pmod p$. We call a square a "quadratic residue".

If $a^2 \equiv b^2$ then $p \mid a^2 - b^2 = (a-b)(a+b)$
so $p \mid a-b$ or $p \mid a+b$ so $a \equiv b$ or $a \equiv -b$
Thus every non zero square is the square of exactly two numbers. Hence there are exactly $\frac{p-1}{2}$ quadratic residues.

1 and 4 are quadratic residues

2 and 3 are quadratic non residues

$p=7$ $\quad 1^2 \equiv (-1)^2 \equiv 1 \quad 2^2 \equiv (-2)^2 \equiv 4 \quad 3^2 \equiv (-3)^2 \equiv 2$

So 1, 2, 4 are squares $\pmod 7$, 3, 5, 6 are not.

2/11/10

Numbers and Sets (16)

Suppose a is a square modulo n, where $n = pq$, p, q prime, and $(a, n) = 1$.
Then a is a square mod p and a square mod q.
$\exists s \quad (\pm s)^2 \equiv a \pmod p \qquad \exists t \quad (\pm t)^2 \equiv a \pmod q$
By CRT we get 4 square roots of $a \pmod n$ corresponding to s, t $-s, -t$
$-s, t$ $s, -t$
[e.g. $c \equiv -s \pmod p$ $c \equiv t \pmod q \Rightarrow c^2 \equiv a \pmod n$]
They come in 2 pairs $\pm u$, $\pm v$
e.g. $4 \equiv (\pm 2)^2 \equiv (\pm 5)^2 \pmod{21}$

Tossing a coin over the phone

Anneka and Brian wish to toss a coin fairly by phone.
A: Chooses two 100 digit primes $p, q \equiv 3 \pmod 4$. Tells B product $n = pq$
B: Picks a number u coprime to n, $a \equiv u^2 \pmod n$
A: Computes the 4 square roots $\pm u, \pm v \pmod n$. Picks a pair and tells Brian.
B: If A picks $\pm u$, B says "You win", A picks $\pm v$, B says "You lose"

Can Brian cheat? If A picks $\pm u$ and B says, "you lose", must produce $\pm v$ as evidence.

To know $\pm v$ is equivalent to factoring n.
Conversely if he can find $\pm v$ he knows $u^2 \equiv v^2 \pmod n \Rightarrow n \mid (u-v)(u+v)$
but $n \nmid u-v$, $n \nmid u+v$ so wlog $p \mid u-v$, $q \mid u+v$ and
$p = (n, u-v)$, $q = (n, u+v)$
It works because it is possible to find 100 digit primes with near certainty (based on random Fermat) and the congruence/power/CRT/hcf calculations are feasible, but factorisation is thought to be unfeasible.

Public key Cryptography

Let us agree to write text messages as strings of numbers, e.g. $A, B, \ldots Z, \Rightarrow 00, \ldots 25$
I wish for people to be able to encrypt messages to me so I can decrypt them but no one else (e.g. a malicious eavesdropper) can do so. So we need an encryption scheme which is public knowledge, but only I can decrypt.

The RSA (Rivest, Shamir, Adleman)

I think of two large primes p, q. Let $n = pq$. Pick e coprime to $\phi(n) = (p-1)(q-1)$
Work out d which is the inverse of $de \equiv 1 \pmod{\phi(n)}$. Publish the pair n, e.

To send me a message, split $M < n$, send $M^e \pmod n$. How do I find M? $(M^e)^d \equiv M^{k\phi(n)+1} \equiv M \pmod n$.
How can a bad guy find M? Finding $\phi(n)$ is as hard as factorising n.
(If he knows $\phi(n)$ then p and q are the roots of $x^2 - (n+1-\phi)x + n = 0$.)
Noone knows if RSA can be broken without factorising n.

Some choices of p and q are less secure.

e.g. $p = 31$, $n = 61$, $n = 1891$, $\phi(n) = 30 \cdot 60 = 1800$

but $M^{30} \equiv 1 \pmod{p} \Rightarrow M^{60} \equiv 1 \pmod{p}$

$M^{60} \equiv 1 \pmod{q} \Rightarrow M^{60} \equiv 1 \pmod{n}$

MMG knew RSA before R, S and A

Real Numbers

The central characteristic of $\mathbb{N}$ is WOP. Formally, can construct via Peano.

$\mathbb{Z}$ is obtained from the natural numbers by allowing subtraction.

$\mathbb{Q}$ is obtained from $\mathbb{Z}$ by allowing division.

Formally; we can construct rationals from the integers in the following way:

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

$(a, b) R (c, d)$ if $ad = bc$, then R is an equivalence relation.

Let $\mathbb{Q}$ be the set of equivalence classes. Write $\frac{a}{b}$ for $[(a, b)]$.

Need to check can define $+, \times, <$ on $\mathbb{Q}$ so defined to make it a totally ordered fie

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) Multiplication is distributive over addition $a(b+c) = ab + ac$

means that $\mathbb{Q}$ is a field.

d) there is an order relation on $\mathbb{Q}$ which is reflexive, antisymmetric, & transitive.

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

make $\mathbb{Q}$ a totally ordered set.

f) The order respects the field i.e. $\forall p, q, r \in \mathbb{Q}$ $\quad p < q, 0 < r \Rightarrow pr < qr$ $\quad p < q \Rightarrow p + r < q + r$

A totally ordered field satisfies a) to f). Note that in any totally ordered field we have $0 < 1$ for otherwise, $1 < 0$ so $1 + (-1) < 0 + (-1)$ so $0 < -1$, $0 < -1 \Rightarrow 0 < (-1)^2 = 1$ ✗

Observe that $\mathbb{Z}_p$ is a field.

But it cannot be ordered: for we would have $0 < 1$, $0 + 1 < 1 + 1$, $\Rightarrow 2 < 3$, $3 < 4$ etc ... $p - 1 < p = 0$ so by transitivity $0 < 0$, a contradiction.

Numbers and Sets (17)

Remark $\mathbb{Q}$ is dense: if $p, q \in \mathbb{Q}$, $p<q$ then $\exists r \in \mathbb{Q}$ with $p<r<q$
But we cannot solve equations in the rationals.

Theorem There is no $q \in \mathbb{Q}$ with $q^2 = 2$.

Proof Suppose not, and $\left(\frac{a}{b}\right)^2 = 2$ where b is as small as possible, so $(a,b)=1$, and $a^2 = 2b^2$.

Proof 1 Since a^2 is even, a is even, then $a=2c$. So $2c^2 = b^2 \Rightarrow b^2$ is even, b is even. Contradiction as $(a,b)=1$.

Proof 2 We know b is a product of primes. Let $p|b$. Then $p|a^2$.
$p|a$, contradicting $(a,b)=1$.

Proof 3 (Dirichlet) 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 $\frac{a}{b} = \frac{2b-a}{a-b}$, which has denominator $< b$ (since $a<2b$), a contradiction.

Proof 4 As proof 3, but pick u, v with $av + bu = 1$. Then $\frac{a}{b}$ is an integer!
False.

Remark To prove there is no rational with $q^2 = 7b$.
Proof 1 hard; Proof 3 uses only the division algorithm.
Proofs 2 and 4 use Bezout, then they are immediate.

So we can split $\mathbb{Q}$ as $\{q \in \mathbb{Q} : q<0 \text{ or } q^2<2\} \cup \{q \in \mathbb{Q} : q>0, q^2>2\}$ with a "pinhole"
The real numbers fill this hole. But we can no longer appeal to intuition.
(e.g. is $0.9999\ldots = 1$?).

Definition The number $S \in \mathbb{R}$ is a least upper bound for the set $S \subseteq \mathbb{R}$ if:
i) S is an upper bound for S i.e. $\forall x \in S$, $x \leq S$
ii) If t is an upper bound for S, then $S \leq t$.

Axiom The central characteristic of $\mathbb{R}$ is the following assumption:
Every non-empty subset of real numbers that has an upper bound has a least upper bound.
By definition, the least upper bound for s is unique. We write

$s = \sup S$, the supremum of S.

Formally, we can construct a set $\mathbb{R}$ for $\mathbb{Q}$ by letting $\mathbb{R}$ be the set of all partitions $L \cup R$ of $\mathbb{Q}$, where $l < r$ for all $l \in L, r \in R$
Inject $\mathbb{Q} \to \mathbb{R}$ by $q \to \{x : x \leq q\} \cup \{x : x > q\}$
Show $\mathbb{R}$ has stated properties. "Dedekind cuts".

Let $a, b \in \mathbb{R}$. Define $[a,b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ "closed interval"
$(a,b) = \{x \in \mathbb{R} : a < x < b\}$ "open interval"

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

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

If S has a maximum element then $\sup S = \max S$, but $\sup S$ can exist even if $\max S$ does not, in which case $\sup S \notin S$.

Theorem (Axiom of Archimedes) Given $r \in \mathbb{R}$, there exists $n \in \mathbb{N}$ with $n > r$.
Proof If not, r is an upper bound for $\mathbb{N}$. Since $\mathbb{N} \neq \emptyset$, $\exists\, S = \sup \mathbb{N}$.
Since S is the sup, $S - 1$ is not an upper bound. Hence there exists $n \in \mathbb{N}$ with $S - 1 < n$, $\Rightarrow S < n + 1 \in \mathbb{N}$, contradicts S being an upper bound for

Notice that every non empty set $S \subseteq \mathbb{R}$ which is bounded below has a greatest lower bound or infimum as $-S = \{-x : x \in S\}$ is non empty and bounded above and $\inf S = -\sup(-S)$.

Corollary if $\{\frac{1}{n} : n \in \mathbb{N}\} = 0$.
Proof Clearly 0 is a lower bound for this set. If $t > 0$, then $\exists\, n \in \mathbb{N}$ with $n > \frac{1}{t}$ (by axiom of Archimedes) so $t > \frac{1}{n}$, but $\frac{1}{n} \in S$, so t is not a lower bound.
Hence there are no infinitely large or infinitesimally small reals.

Axiom of Archimedes: $\forall r\ \exists n \in \mathbb{N},\ n \geq r$
Corollary: $\inf\{\frac{1}{n} : n \in \mathbb{N}\} = 0$

We can now see that $\mathbb{Q}$ is dense in $\mathbb{R}$:
i.e $\forall r, s \in \mathbb{R}\ \exists q \in \mathbb{Q},\ r < q < s$
By the corollary there exists $n \in \mathbb{N}$ with $\frac{1}{n} < s - r$
By the axiom of Archimedes $\exists N \in \mathbb{N}$ with $N > s$. Let $T = \{k \in \mathbb{N} : \frac{k}{n} \geq s\}$. Since $Nn \in T$, we have $T \neq \emptyset$, so by WOP there is a least element $m \in T$. Let $q = \frac{m-1}{n}$

Since $m - 1 \in T$, $q < s$. If $q \leq r$, then $\frac{m}{n} = q + \frac{1}{n} < r + (s - r) < s$ contradicting $m \in T$.
Hence $r < q < s$.

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

Proof Let $S = \{r \in \mathbb{R} : r^2 \leq 2\}$. Then $0 \in S$, so $S \neq \emptyset$ and $r \leq 3\ \forall r \in S$. So S is bounded above by 3. Hence $x = \sup S$ exists, and $0 \leq x \leq 3$.

Suppose $x^2 < 2$. Let $0 < t < 1$. Then
$(x+t)^2 = x^2 + 2tx + t^2 \leq x^2 + 6t + t = x^2 + 7t$
Pick $t < \frac{(2 - x^2)}{7}$, with $0 < t < 1$. Then $(x+t)^2 < 2$
Shows that $x + t \in S$, contradicting x being an upper bound.

Suppose $x^2 > 2$. Let $0 < t < 1$. Then
$(x - t)^2 = x^2 - 2tx + t^2 \geq x^2 - 6t$. Pick $t < \frac{x^2 - 2}{6}$ with $0 < t < 1$. Then $(x-t)^2 > 2$, so $x - t$ is an upper bound for S, contradicting x as the least upper bound.

So $x^2 = 2$ □

Sequences A sequence is a function $\mathbb{N} \to \mathbb{R}$. If $a : \mathbb{N} \to \mathbb{R}$ then we usually write $a_1, a_2, a_3 \ldots$ instead of $a(1), a(2), a(3)$.
What does it mean for a sequence to tend to a limit?

Definition The sequence $(a_n)_{n=1}^{\infty}$ tends to the limit L as $n \to \infty$ if, for every positive ε, $\exists\ N \in \mathbb{N}$ such that $\forall n > N$, $|a_n - L| < \varepsilon$ holds.

Symbolically $\forall \varepsilon > 0\ \exists N\ \forall n > N\ |a_n - L| < \varepsilon$
Also "$a_n \to L$ as $n \to \infty$"

or $\lim_{n \to \infty} a_n = L$ or "a_n converges to L".

If L exists but we don't know its value, we might just say "a_n converges".

"Diverges" means "Doesn't converge". Examples:

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

Given $\varepsilon > 0$, choose $N > \frac{1}{\varepsilon}$ (Archimedes Axiom).

If $n > N$, $|a_n - 1| = \frac{1}{n} < \varepsilon$. Hence $a_n \to 1$.

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

Given an $\varepsilon > 0$, choose $N > \frac{1}{\varepsilon}$. If $n > N$ then $|a_n - 0| \leq \frac{1}{n} < \varepsilon$

Hence $a_n \to 0$

The definition of $a_n \not\to L$ is $\exists \varepsilon > 0 \ \forall N \ \exists n \geq N \ |a_n - L| \geq \varepsilon$

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

Let $L \in \mathbb{R}$ be a potential limit. Let $\varepsilon = \frac{1}{2}$. Let $N \in \mathbb{N}$. If $L \geq 0$ pick $n \in \mathbb{N}$, $n > N$, n even. If $L \leq 0$ pick $n > N$, n odd. Then $|a_n - L| \geq \varepsilon$ So (for any $L \in \mathbb{R}$) $a_n \not\to L$. Hence (a_n) diverges.

The following is used constantly.

"Monotonic" means either increasing or decreasing

Theorem Every bounded, monotonic sequence converges.

Proof Suppose a_n is increasing; i.e. $a_{n+1} \geq a_n \ \forall n$. The set $\{a_n : n \geq 1\}$ is bounded above so it has a supremum, say L. Given $\varepsilon > 0$, then $L - \varepsilon$ is not an upper bound for the set, so there exists N with $a_N > L - \varepsilon$. Since a_n is increasing, $a_n > L - \varepsilon \ \forall n > N$. Thus $L - \varepsilon < a_n \leq L \ \forall n \geq N$ implying $|a_n - L| < \varepsilon$. Hence $a_n \to L$.

Decreasing case is very similar.

Remarks i) $a_n = n$ is not bounded and diverges

ii) Theorem is in fact equivalent to our axiom.

Something like $a_2, a_3, a_5, a_{11}, a_{17}$ is a subsequence of (a_n)

Formally a subsequence is a sequence $a_{g(n)}$ where $g : \mathbb{N} \to \mathbb{N}$ is a strictly increasing function.

Theorem Every sequence has a monotonic subsequence.

Proof Call a_k a high point if $a_k \geq a_n \ \forall n \geq k$. If there are infinitely many high points they form a decreasing subsequence. If there are only finitely many high points, there exists N so no a_n with $n > N$ is a high point. So pick a subsequence $N' > N$ with $a_{N'} > a_N$ (since a_N is not a high point) then $N'' > N'$, etc. Carry on to construct an increasing subsequence $a_N, a_{N'}, a_{N''}, \ldots$ etc.

19/11/10

Numbers and Sets (19)

$a_n \to L$ means $\forall \varepsilon > 0 \ \exists N \ \forall n > N \ |a_n - L| < \varepsilon$

Recall the triangle inequality $|x+y| \leq |x| + |y|$

Theorem

i) If $a_n \to a$, and $a_n \to b$, then $b = a$ (limits are unique)
ii) If $a_n \to a$ and $b_n = a_n$ except for finitely many n, then $b_n \to a$.
iii) If $a_n = a$ for all n then $a_n \to a$
iv) If $a_n \to a$, $b_n \to b$ then $(a_n + b_n) \to (a+b)$
v) If $a_n \to a$, $b_n \to b$ then $a_n b_n \to ab$

vi) If $a_n \to a \neq 0$ and $a_n \neq 0 \ \forall n$ then $\frac{1}{a_n} \to \frac{1}{a}$
vii) (sandwich theorem) if $a_n \to a$, $b_n \to a$, $a_n \leq c_n \leq b_n$ then $c_n \to a$

Proofs

i) Suppose $a < b$. Let $\varepsilon = \frac{b-a}{2}$. Then there exists N_1 so $|a_n - a| < \varepsilon \ \forall n > N_1$ and N_2, $|a_n - b| < \varepsilon \ \forall n > N_2$

Pick $n > \max\{N_1, N_2\}$. Then:
$|a-b| \leq |a - a_n| + |a_n - b| < \varepsilon + \varepsilon = 2\varepsilon$, contradiction #

ii) There exists K so $a_n = b_n$ if $n > K$. Let $\varepsilon > 0$. There exists N_1 so that $|a_n - a| < \varepsilon$ for $n > N_1$. Let $N = \max\{N_1, K\}$. Then if $n > N$, $|b_n - a| = |a_n - a| < \varepsilon$. Hence $b_n \to a$.

iii) For any $\varepsilon > 0$ we can take $N = 1$.

iv) Let $\varepsilon > 0$. There exists N_1 so that $|a_n - a| < \frac{\varepsilon}{2} \ \forall n > N_1$. There exists N_2 so that $|b_n - b| < \frac{\varepsilon}{2} \ \forall n > N_2$. $N = \max\{N_1, N_2\}$
Then $\forall n > N$
$|(a_n + b_n) - (a+b)| \leq |a_n - a| + |b_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$
Hence $(a_n + b_n) \to (a+b)$

v) Let $\varepsilon > 0$. There exist N_1, N_2, N_3 so $|a_n - a| < \frac{\varepsilon}{2(|b|+1)}$ for $n > N_1$, $|b_n - b| < \frac{\varepsilon}{2(|a|+1)}$ for $n > N_2$, $|b_n - b| < 1$ for $n > N_3$

($|b_n| < |b| + 1$)

Let $N = \max\{N_1, N_2, N_3\}$. Then for $n > N$
$|a_n b_n - ab| = |b_n(a_n - a) + a(b_n - b)| \leq |b_n||a_n - a| + |a||b_n - b|$
$< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, so $a_n b_n \to ab$

vi) Let $\varepsilon > 0$. Then $\exists N_1, N_2$ so $|a_n - a| < \varepsilon \frac{|a|^2}{2}$ for $n > N_1$ and $|a_n - a| < \frac{|a|}{2}$ for $n > N_2$ (so $|a_n| > \frac{|a|}{2}$).
Let $N = \max\{N_1, N_2\}$. Then for all $n > N$

$\left|\frac{1}{a_n} - \frac{1}{a}\right| = \frac{|a_n - a|}{|a_n||a|} < \frac{2|a_n - a|}{|a|^2} < \varepsilon$, so $\frac{1}{a_n} \to \frac{1}{a}$

(ii) (v)

vii) by (iii) and (iv) $b_n - a_n \to 0$ Let $\varepsilon > 0$. Then there exists N with $|b_n - a_n| < \varepsilon$ for all $n > N$
$|c_n - a_n| < \varepsilon$ for all $n > N$, Hence $c_n - a_n \to 0$
$\Rightarrow c_n \to a$ □

Examples $x_n = \frac{n^2(n+1)(2n+1)}{n^4+1}$, so $x_n = \frac{(1+\frac{1}{n})(2+\frac{1}{n})}{1+\frac{1}{n^4}} \to \frac{1\cdot 2}{1} = 2$ by (iii) & (v)

$y_n = \frac{100^n}{n!}$, $\frac{y_{n+1}}{y_n} = \frac{100}{n+1} < \frac{1}{2}$ if $n \geq 200$

So $0 < y_n < y_{200} \cdot \frac{2^{200}}{2^n} < y_{200} \cdot \frac{2^{200}}{n}$ if $n > 200$

by (ii), (vii) $y_n \to 0$.

$x_1 = 1$, $x_{n+1} = \frac{x_n^2+1}{3}$, $n \geq 1$. Then $x_n \geq \frac{1}{3}$ for all n. $x_2 = \frac{2}{3} < x_1$

$x_{n+1} - x_n = \frac{x_n^2+1}{3} - \frac{x_{n-1}^2+1}{3} = \frac{(x_n + x_{n-1})(x_n - x_{n-1})}{3}$

So $x_n < x_{n-1} \Rightarrow x_{n+1} < x_n$ so x_n decreases, by induction.
Since $x_n \leq \frac{1}{3}$, (x_n) is monotonic and bounded (so by theorem) $x_n \to L$ for some
$x_{n+1} \to L$, $L = \frac{L^2+1}{3}$ so $L = \frac{3}{2} \pm \frac{1}{2}\sqrt{5}$,
since $\frac{1}{3} \leq x_n \leq L$ we have $x_n \to \frac{3-\sqrt{5}}{2}$

Series In a field, the sum of two numbers is defined, so by induction, the sum of finitely many is defined. Infinite sums are not defined.
Let (a_n) be a sequence. Then $S_m = \sum_{n=1}^{m} a_n$ is the m^{th} partial sum of the series whose n^{th} term is a_n.
$\sum_{n=1}^{\infty} a_n = \lim_{m\to\infty} S_m$ if the limit exists.

Examples i) $a_n = \frac{1}{n(n-1)}$, $n \geq 2$. $S_m = \sum_{n=2}^{m} \frac{1}{n(n-1)} = \sum_{n=2}^{m} \left\{\frac{1}{n-1} - \frac{1}{n}\right\} = 1 - \frac{1}{m} \to 1$ as $m \to \infty$
$\therefore S_\infty = 1$.

ii) $a_n = \frac{1}{n^2}$, $S_m = \sum_{n=1}^{m} \frac{1}{n^2}$. Then S_m is increasing and $S_m = 1 + \sum_{n=2}^{m} \frac{1}{n(n-1)} < 2$
S_m Increases and is bounded above so it converges to a limit ≤ 2.

iii) $a_n = r^n$, $|r| < 1$, $S_m = r\frac{1-r^m}{1-r} \to \frac{r}{1-r}$ since $r^m \to 0$, $S_\infty = \frac{r}{1-r}$

iv) $a_n = \frac{1}{n}$. $S_{2^k} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^k} \geq 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \ldots + \frac{1}{2^k}$
$= 1 + \frac{k}{2}$
Hence S_m is unbounded so $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

22/11/10

Numbers and Sets (20)

Decimal Expansions

Let (d_n) be a sequence of numbers with $d_n \in \{0,1,\dots,9\}$. Then $\sum_{n=1}^{\infty} \frac{d_n}{10^n}$ converges to a limit r, $0 \le r \le 1$ because the partial sums $S_m = \sum_{n=1}^{m} \frac{d_n}{10^n}$ 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 that $r = 0 \cdot d_1 d_2 d_3 \dots$ is the decimal expansion of r.

Does every x $0 \le x \le 1$ have a decimal expansion? Pick d_1 maximal so $\frac{d_1}{10} \le x < 1$, so $d_1 \le 9$ and $0 \le x - \frac{d_1}{10} < \frac{1}{10}$
d_2 max so $\frac{d_2}{100} \le x - \frac{d_1}{10} < \frac{1}{10}$, so $d_2 \le 9$ and $0 \le x - \frac{d_1}{10} - \frac{d_2}{100} < \frac{1}{100}$
Inductively pick $\frac{d_n}{10^n} \le x - \sum_{j=1}^{n-1} \frac{d_j}{10^j} < \frac{1}{10^{n-1}}$, so $0 \le x - \sum_{j=1}^{n} \frac{d_j}{10^j} < \frac{1}{10^n}$

$x - \sum_{j=1}^{n} \frac{d_j}{10^j}$ is sandwiched between 0 and $\frac{1}{10^n} \to 0$ so $x = 0 \cdot d_1 d_2 d_3 \dots$
Can we have $0 \cdot a_1 a_2 a_3 \dots = 0 \cdot b_1 b_2 b_3 \dots$?
Say $a_j = b_j$ for $j < k$ and $a_k < b_k$. Then $\sum_{j=k+1}^{\infty} \frac{a_j}{10^j} \le \sum_{j=k+1}^{\infty} \frac{9}{10^j} = \frac{1}{10^k}$
so we must have $b_k = a_k + 1$, $a_k = 9$ $j > k$, $b_j = 0$ $j > k$.

A decimal is periodic if after a finite number of digits it repeats in blocks of k: i.e. $d_{k+n} = d_n$ for $n > l$, e.g. $x = 0 \cdot 7643\,157\,157\,157\dots$
Clearly a periodic decimal is rational eg. $10^4 x - 7643 = 0 \cdot 157\,157\,157$
$10^4 x - 7643 = 157 \sum_{j \ge 1} \frac{1}{10^{3j}} = \frac{157}{10^3} \cdot \frac{1}{1-10^{-3}} \in \mathbb{Q}$.

Conversely, if x is rational then x has a periodic decimal expansion. For suppose $x = \frac{p}{2^a 5^b q}$ where $(q, 10) = 1$. Then $10^{\max(a,b)} x = \frac{e}{q} = n + \frac{f}{q}$ where $e, n, f \in \mathbb{Z}$, and $0 \le f < q$. By Fermat-Euler:
$10^{\varphi(q)} \equiv 1 \pmod{q}$ i.e. $10^{\varphi(q)} - 1 = kq$, $k \in \mathbb{N}$. $\frac{f}{q} = \frac{kf}{kq} = \frac{kf}{10^{\varphi}-1}$

$= kf \sum_{j \ge 1} \frac{1}{10^{\varphi j}}$. Since $kf < kq$, we can write kf as a φ digit number $kf = d_1 d_2 \dots d_\varphi$ so $\frac{f}{q}$ is a repeating decimal $0 \cdot d_1 \dots d_\varphi d_1 \dots$
Shift to the right, x is periodic.

A number $x \in \mathbb{R}$ is irrational if it is not rational, $x \notin \mathbb{Q}$.
e.g. $x = 0 \cdot 01101010001010\dots$ with 1s in prime positions is irrational since for every k there is a block of more than k zeros. Likewise:
$x = 0 \cdot 2357\,11\,13\,17\,19\dots$ is irrational because for every L and k we can choose t so that $10^{tk-1} > L$ and a prime $10^{tk-1} \le p < 10^{tk}$ having tk digits. Then x cannot repeat after L digits with period k otherwise $p = d_1 \dots d_k d_1 \dots d_k$ is not prime.

We define $e = \sum_{j=0}^{\infty} \frac{1}{j!}$. Note that the limit exists because the partial sums are increasing, $\le 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \dots = 3$
Is e a rational number?
Suppose $e = \frac{p}{q}$. $2 < e < 3$ so $q \ge 2$. Then $q!\,e \in \mathbb{N}$.

But $q!\,e = q! + q! + \frac{q!}{2!} + \dots + \frac{q!}{q!} + \frac{q!}{(q+1)!} + \dots$
$q!\,e = N + x$ where $N \in \mathbb{N}$ $x = \frac{1}{\dots} + \frac{1}{\dots} + \dots$

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

Since $0 < x < 1$ this contradicts $q!e = N + x \in \mathbb{N}$

An algebraic number is the root of a polynomial with integer coefficients, (or rational coefficients). Rationals are algebraic: $x = \frac{p}{q}$ is a root of $qx - p = 0$. $\sqrt{2}$ a root of $x^2 - 2 = 0$. A number is transcendental if it is not algebraic. Do transcendental numbers exist?

Let $L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000010\ldots$ ⇒ has a 1 in every $(n!)^{th}$ place

Theorem (Liouville, 1851) L is transcendental.

Proof Suppose $f(L) = 0$ where $f(x) = a_k x^k + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$

Let $C = k|a_k| + (k-1)|a_{k-1}| + \cdots + |a_1|$

Pick $m \in \mathbb{N}$ so $m \geq k$ and $10^{m!} > \frac{10C}{q}$

Let $S = \sum_{j=1}^{m} \frac{1}{10^{j!}}$ so $S = \frac{p}{q}$, $p \in \mathbb{Z}$, $q = 10^{m!}$

We may assume $f(S) \neq 0$ since f has finitely many roots and can increase m to avoid $f(S) = 0$.

Then $L - S = \sum_{j=m+1}^{\infty} \frac{1}{10^{j!}} \leq \frac{1}{10^{(m+1)!}} \sum_{n \geq 0}^{\infty} \frac{1}{10^n} = \frac{10}{9q^{(m+1)!}} < \frac{1}{Cq^{m+1}} < \frac{1}{Cq^k}$

24/11/10

Numbers and Sets (21)

$a_i \in \mathbb{Z}$

$L = \sum_{n \geq 1} \frac{1}{10^{n!}}$ is transcendental. $f(L) = 0$, $f(x) = a_k x^k + \dots + a_1 k + a_0$

$C = k|a_k| + \dots + |a_1|$ $\quad n \in \mathbb{N}, n \geq k, \quad 10^{n!} \geq \frac{10C}{q}$ $\quad S = \frac{p}{q}, q = 10^n$

$S = \sum_{j=1}^{n} \frac{1}{10^{j!}}$ $\quad L - S = \frac{1}{10^{(n+1)!}} \sum_{m \geq n} \frac{1}{10^m} = \frac{10}{q q^{(n+1)!}} < \frac{1}{C q^{n+1}} < \frac{1}{C q^k}$

$f(S) \neq 0$. Clearly $0 < S < L < 1$ so for all $n \in \mathbb{N}$

$0 < L^n - S^n = (L-S)(L^{n-1} + SL^{n-2} + \dots + S^{n-1}) < n(L-S)$

Since $S = \frac{p}{q}$ and $f(S) \neq 0$, we have $|f(S)| \geq \frac{1}{q^k}$.

$$\frac{1}{q^k} \leq |f(S)| = |f(S) - f(L)| = \left|\sum_{n=0}^{k} a_n (S^n - L^n)\right| \leq \sum_{n=0}^{k} |a_n| n |L-S|$$

$$= (L-S)C < \frac{1}{q^k} \quad \# \text{ a contradiction} \quad \square$$

Countability!!! We counted sets by constructing bijections with known sets, normally with $[n] = \{1, 2, \dots, n\}$.

Lemma If $f : [n] \to [n]$ is injective then it is also surjective (therefore bijective)

Proofs By induction on n. True for $n = 1$, if $i \neq j$.

Let $n > 1$. Let $j = f(n)$. Let $g : [n] \to [n]$ be $g(j) = n$, $g(n) = j$, $g(i) = i$

Then g is a bijection. The map $g \circ f : [n] \to [n]$ is injective and $g \circ f(n) = n$.

So the map $h : [n-1] \to [n-1]$, $h(i) = g \circ f(i)$ exists and is injective

so by induction hypothesis, is surjective. Hence $g \circ f$ is surjective. Hence, so is f. $\square$

Corollary If A is a set and $f : A \to [n]$, $g : A \to [m]$ are bijections, then $n = m$.

Proofs We may suppose $m \geq n$. Let h be $h : [n] \to [m]$, $h(i) = i$. Then

$[n] \xrightarrow{g^{-1}} A \xrightarrow{f} [n] \xrightarrow{h} [m]$ is injective. By the lemma it is surjective. So

h is surjective, $m = n$ $\square$

Definition The set A is finite if $\exists n \in \mathbb{N}_0$ with a bijection from $A \to [n]$. The size of A, $|A|$ is n. By the corollary, the size of A is well defined.

What about infinite sets?

Lemma Let $S \in \mathbb{N}$. Then either S is finite, or there is a bijection $g : \mathbb{N} \to S$

Remarks g "counts" S.

Proofs If $S \neq \emptyset$, then by WOP it has a least element $s_1 \in S$. If $S \setminus \{s_1\} \neq \emptyset$ it has a least element s_2. If $S \setminus \{s_1, s_2\} \neq \emptyset$ it has a least element s_3 and so on. If at some point the process stops, then $S = \{s_1, \dots, s_n\}$ is finite. Otherwise, $g(i) = s_i$, $g : \mathbb{N} \to S$ is well defined; each i has a unique s_i, and g 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 so $g(i) = k$ for some $i \leq k$. $\square$

Definition The set A is countable if it is finite, or there is a bijection between A and $\mathbb{N}$.

Theorem The following are equivalent:

i) A is countable
ii) There is an injection of $A \to \mathbb{N}$
iii) $A = \emptyset$ or there is a surjection $\mathbb{N} \to A$

Proof Plainly (i) $\Rightarrow$ (ii). Conversely, if there is an injection $f : A \to \mathbb{N}$, then f gives a bijection between A and $S = f(A)$. If S is finite then so is A. If S is infinite, there is a bijection $S \to \mathbb{N}$ (by Lemma), so $A \to \mathbb{N}$ is a bijection. Either way A is countable so (ii) $\Rightarrow$ (i).

Plainly (i) $\Rightarrow$ (iii). Conversely, if $A \neq \emptyset$ and there is a surjection $f : \mathbb{N} \to A$ define a map $g : A \to \mathbb{N}$ by $g(a) = \min f^{-1}\{a\}$ which exists by WOP. Then g is an injection so by (ii) A is countable, hence (iii) $\Rightarrow$ (i).

Example

$$f(n) = \begin{cases} 2n & n > 0 \\ 2(-n)+1 & n \leq 0 \end{cases}$$

$f : \mathbb{Z} \to \mathbb{N}$ a bijection $\Rightarrow$ $\mathbb{Z}$ is countable.

26/11/10

Numbers and Sets (22)

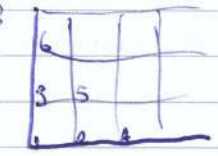
Definition: Set is countable $\Leftrightarrow$ finite or bijects with $\mathbb{N}$

Theorem: i) A countable
ii) $\exists$ injection $A \to \mathbb{N}$
iii) $\exists$ injection $\mathbb{N} \to A$ (or $A = \emptyset$)

$\mathbb{Z}$ is countable.

$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ $\quad (a,b) = 2^a 3^b$ is injective, hence $\mathbb{N} \times \mathbb{N}$ is countable.

In fact, we can give an explicit bijection:



$(a,b) \mapsto \binom{a+b}{2} - a + 1$

Since $\mathbb{Z}$ is countable we have an injection $\mathbb{Z} \to \mathbb{N}$. So there are injections $\mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ because $\mathbb{Z}$ and $\mathbb{N} \times \mathbb{N}$ are both countable, so $\mathbb{Z} \times \mathbb{Z}$ is countable.

If $A \to B$ is injective and B is countable then A is countable since we can inject A to $\mathbb{N}$

$\mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ $\quad \frac{p}{q} \mapsto (p,q)$, $(p,q) = 1$, injective, $q > 0$.
$0 \mapsto (0,0)$ so $\mathbb{Q}$ is countable.

$\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is countable, since we can inject $\mathbb{Z}^3 \to \mathbb{N}^2 \to \mathbb{N}$
By induction $\mathbb{Z}^k$ is countable, where $k \in \mathbb{N}$.

Theorem A countable union of countable sets is countable.

Proof Let I be a countable index set. For each $\alpha \in I$ let A_α be a countable set. We want to show $A = \bigcup_{\alpha \in I} A_\alpha$ is countable.
Since I is countable there is a bijection $f: I \to [n]$ for some n or $f: I \to \mathbb{N}$
So we may relabel $A_1, A_2 \dots A_n$ or $A_1, A_2, A_3 \dots$ (using label f_α instead of α_i)

Hence $A = \bigcup_{j \geq 1} A_j$. For each A_j there is an injection $g_j : A_j \to \mathbb{N}$.

For each $a \in A$ let $m_a = \min\{j : a \in A_j\}$ (exists by WOP)
Then:
$a \mapsto (m_a, g_{m_a}(a))$ is an injection $A \to \mathbb{N} \times \mathbb{N}$ so A is countable ∎

Example $\mathbb{Q} = \bigcup_{n \geq 1} \frac{1}{n}\mathbb{Z} = \bigcup_{n \geq 1} \left\{\frac{m}{n} : m \in \mathbb{Z}\right\}$ so again $\mathbb{Q}$ is countable.

Theorem The set of algebraic numbers is countable.

Proof Let P_k be the set of polynomials of degree k with integer coefficients

The map $a_k x^k + a_{k-1} x^{k-1} + \dots + a_0 \mapsto (a_k, a_{k-1}, \dots, a_0)$
$P_k \to \mathbb{Z}^{k+1}$ is an injection.
Let P be the set of all polynomials with integer coefficients. Then $P = \bigcup_{k \geq 1} P_k$ is a countable union of countable sets. For each polynomial $p \in P$ let R_p be the set of its roots. Then R_p is finite. Thus the union $\bigcup_{p \in P} R_p$ is the set of algebraic numbers and is a countable union of countable sets, so is countable ∎

→ Not countable

Are there uncountable sets? Yes.

Theorem $\mathbb{R}$ is uncountable.

Proof Suppose $\mathbb{R}$ is countable, then we can list the reals as $r_1, r_2, r_3, \ldots$
Write each r_n in decimal form (unique decimals, never use $0.999\ldots$)

$r_1 = n_1 \cdot d_{11}\, d_{12}\, d_{13} \ldots$
$r_2 = n_2 \cdot d_{21}\, d_{22}\, d_{23} \ldots$
$r_3 = n_3 \cdot d_{31}\, d_{32}\, d_{33} \ldots$

$d_n = \begin{cases} 0 & \text{if } d_{nn} \neq 0 \\ 1 & \text{if } d_{nn} = 0 \end{cases}$

Write $r = 0 \cdot d_1 d_2 d_3 \ldots$, a real number not listed, because for all n, $r \neq r_n$ as d_n is clearly different.
This is the diagonal argument of Cantor (1783).

Corollary There are uncountably many transcendental numbers.

29/11/10

Numbers and Sets (23)

$\mathbb{R}$ is uncountable $\therefore$ transcendental numbers are uncountable
$\mathbb{R}$ = transcendentals $\cup$ algebraics
If the transcendentals were countable, then $\mathbb{R}$, as a (finite) union of countable sets would also be countable, but we know this is not the case.

Recall: $\mathcal{P}X = \{Y : Y \subset X\}$
Suppose $\mathcal{P}\mathbb{N}$ were countable, then $S_1, S_2, S_3, S_4, \ldots$ is a list of all subsets of $\mathbb{N}$. Let $S = \{n : n \notin S_n\}$. Then S is not in the list.
(Where is S? Is $S = S_{47}$?) Hence $\mathcal{P}\mathbb{N}$ is uncountable. (diagonal argument).

Let Σ be the set of all functions $\mathbb{N} \to \mathbb{N}$. If Σ were countable we could list its members f_1, f_2, f_3 but then f given by $f(n) = \begin{cases} 1 & f_n(n) \neq 1 \\ 2 & f_n(n) = 1 \end{cases}$
is not in the list. Hence Σ is uncountable.

Alternatively, 0-1 sequences are just indicator functions of subsets of $\mathbb{N}$: add 1 everywhere to get an injection $\mathcal{P}\mathbb{N} \to \Sigma$ (If Σ is countable then so is $\mathcal{P}\mathbb{N}$#

Let $\Sigma^* \subset \Sigma$ be the set of bijections $\mathbb{N} \to \mathbb{N}$. Then Σ^* is uncountable.
Even $\Sigma^{**} \in \Sigma^*$ is uncountable, where for each n, either
i) $f(2n-1) = f(2n-1)$, $f(2n) = f(2n)$
ii) $f(2n-1) = 2n$, $f(2n) = 2n-1$
because each such f is encoded by a 0-1 sequence $(a_n)_{n=1}^{\infty}$ where $a_n = 0$ if (i) holds, and 1 if (ii) holds.
This gives an injection $\Sigma^{**} \leftarrow$ 0-1 sequences $\leftarrow \mathcal{P}\mathbb{N}$.

In some sense $\mathbb{R}$ is "more infinite" than $\mathbb{N}$. We say A, B "have the same cardinality" if there is a bijection between them, $A \to B$. We say $\mathbb{N}$ has cardinality $\aleph_0$, the smallest infinite cardinality. We say $\mathbb{R}$ has cardinality $\mathfrak{c}$, the cardinality of the continuum.

Theorem Let A be a set. Then, there is no surjection $A \to \mathcal{P}A$
Proof Suppose instead that $f: A \to \mathcal{P}A$ is surjective. Let $S = \{a \in A : a \notin f(a)\}$
Since f is surjective, then there exists $s \in A$ with $f(s) = S$.
If so, $s \notin S$ by definition. Likewise, if $s \notin S$ then $s \in S$ by definition. # So f cannot exist $\square$
Hence the cardinality of $\mathcal{P}A$ is "greater" than that of A, and there must be infinitely many different cardinalities.

Constructing bijections directly is sometimes possible: e.g.
$(0,1) \to (1,\infty)$, $x \mapsto \frac{1}{x}$ is bijective
$(0,1) \to (0,\infty)$, $x \mapsto \frac{1}{x} - 1$ is also bijective

$(-1,1) \to \mathbb{R}$ $\quad x \mapsto \begin{cases} \frac{1}{x} - 1 & x > 0 \\ 0 & x = 0 \\ \frac{1}{x} + 1 & x < 0 \end{cases}$

$(0,1) \leftrightarrow (-1,1)$ $\quad x \mapsto 2x - 1$

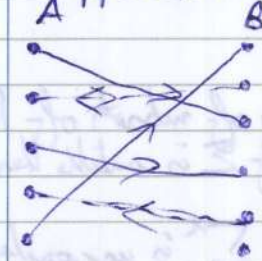
So $(0,1)$ has cardinality.

What is the cardinality of $\mathcal{P}\mathbb{N}$? Since there is a bijection $\mathbb{Q} \leftrightarrow \mathbb{N}$ there is a bijection $\mathcal{P}\mathbb{Q}$ to $\mathcal{P}\mathbb{N}$. The map $r \to \{q \in \mathbb{Q} : q \le r\}$ is an injection $\mathbb{R} \to \mathcal{P}\mathbb{Q}$

The map $\mathcal{P}\mathbb{N} \to \mathbb{R}$ $\quad S \mapsto 0.i_S(1)\, i_S(2)\, i_S(3)\ldots$ is injective, where i_S is the indicator function of S.

Theorem (Schröder-Bernstein or Cantor-Bernstein Theorem)
Suppose the are injections $A \to B$ and $B \to A$. Then there is a bijection $A \to B$.

Proof



$f : A \to B$ $\quad g : B \to A$

Define a relation $\sim$ on $A \cup B$ by $x \sim y$ if there is a directive path (path of finite, including 0 length)
Then $\sim$ is an equivalence relation.
(Transitive because f and g are injective maps)
Equivalence classes are:

- finite: hence cycle — $h : A \to B$ $\quad h = f$
- or a two way infinite path — $h = f$
- or a one way infinite path — $h = f$ or g^{-1} depending on start path

01/12/10

Numbers and Sets (24)

Bertrand's Postulate

Bertrand (1845) postulated that there is always a prime between n and $2n$. The primes 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503 shows this is true for $n \leq 2^{11} = 2048$

Bertand verified it for $n < 3 \times 10^6$. Chebyshev (1850) proved it. Ramanujan (1919) gave a simpler proof based on the Gamma Function.

$$\Gamma(z) = \int_0^\infty e^t t^{z-1}\, dt \qquad \Gamma(n+1) = n!$$

Erdös (1932) gave a very simple proof.

$\binom{n}{k+1} / \binom{n}{k} = \frac{n-k}{k+1}$. It is evident that $\binom{n}{k}$ increases in k while $k < \frac{n}{2}$ and decreases while $k > \frac{n}{2}$

In particular $\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}$

Lemma If p is prime and $p^k \mid \binom{2n}{n}$ then $p^k \leq 2n$

Proof We know that the power of p dividing $n!$ is $\sum_{i \geq 1} \lfloor \frac{n}{p^i} \rfloor$

(power of p dividing $\binom{2n}{n}$)

Let L be the largest power of p with $p^L \leq 2n$. Then $k \leq \sum_{i \geq 1} \lfloor \frac{2n}{p^i} \rfloor - 2\sum_{i \geq 1} \lfloor$

$$k \leq \sum_{i \geq 1}^{L} \lfloor \frac{2n}{p^i} \rfloor - 2\lfloor \frac{n}{p^i} \rfloor \quad \text{only } i \leq L \text{ gives non zero terms}$$

$$\leq \sum_{i=1}^{L} 1 = L, \text{ so } k \leq L \qquad \square$$

Lemma For all $m \in \mathbb{N}$, $\prod_{p \leq m} p \leq 4^m$, product over all primes $\leq m$

Proof Easily true for $m \leq 2$. Proceed by induction.

If $m > 2$ is even then $\prod_{p \leq m} p = \prod_{p \leq m-1} p \leq 4^{m-1} < 4^m$ by induct hypothes

If $m = 2k+1$, all the primes in the range $k+2 \leq p \leq 2k+1$ divide $\binom{2k+1}{k}$

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

By the induction hypothesis $\prod_{p \leq m} p = \prod_{p \leq k+1} p \prod_{k+2 \leq p \leq m} p = 4^{k+1} 4^k = 4^m$

Theorem For all $n \in \mathbb{N}$ there is a prime $n < p \leq 2n$.

Proof The prime factors of $\binom{2n}{n}$ are all $< 2n$. If theorem fails, they all $\leq n$. Crucial fact: There is no prime factor with $\frac{2n}{3} < p \leq n$, for such a prime divides $n!$ exactly once, and $(2n)!$ exactly twice.

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, since p^2 doesn't appear in $(2n)!$.
Hence

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq (2n)^{\sqrt{2n}} \prod_{p \leq \frac{2n}{3}} p$$

$$\leq (2n)^{\sqrt{2n}}\, 4^{\frac{2n}{3}}$$

This fails if n is large. Indeed we have

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

$$(2n+1) \leq (2n)^2 \leq (2n)^{\frac{2n}{3}} \quad \text{for } n \geq 14$$

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

or $4^n \leq (2n)^{4\sqrt{2n}}$ Put $r = \sqrt{2n}$ so $r^2 = 2n$

$$4^{\frac{r^2}{2}} \leq r^{8r} \quad \text{or} \quad 2^r \leq r^8$$ This fails if $r = 2^6$ or larger.

So the proof works if $n \geq 2^{11}$. Examples show it works for smaller n.

Let $\pi(x)$ be the number of primes $\leq x$. Euclid shows $\pi(x) \geq \log\log x$
Erdös shows $\pi(x) \geq \log x$. PMT says $\pi(x) \sim \frac{x}{\log x}$
We can almost get this:
First lemma implies $4^x \geq \prod_{\sqrt{x} < p \leq x} p > \sqrt{x}^{\pi(x) - \pi(\sqrt{x})}$

Logs: $\pi(x) \leq \frac{4x}{\log x} + \pi(\sqrt{x}) \leq \frac{4x}{\log_2 x} + \sqrt{x} \leq \frac{5x}{\log_2 x}$

Conversely $\binom{2n+2}{n+1} = \frac{2(2n+1)}{n+1}\binom{2n}{n} \leq 4\binom{2n}{n}$
So pick n with $\frac{x}{4} \leq \binom{2n}{n} \leq x$. Then $\pi(x) \geq \pi\binom{2n}{n} \geq \frac{\binom{2n}{n}}{2n}$ (first lemma)
so $\pi(x) \geq \frac{x}{8n}$
Since $x > \binom{2n}{n} \geq \frac{2^{2n}}{2n+1} > 2^n$, $n \leq \log_2 x$

$$\frac{5x}{\log_2 x} \geq \pi(x) \geq \frac{x}{8\log_2 x}$$