Introduction to the Course

Math = science of patterns
- kinds of patterns = kinds/branches of math
- science of relationships and understanding of these
- carrier of conceptual properties
  mathematics makes invisible visible, abstract concrete, phenomena applicable/explicative (e.g., aerodynamics)
It is about thinking (think outside-the-box)  
  second principles, think about problems in a certain way
  go slower  
  reflection > completion
  goal, understanding  
  often never sure if right
  second principles is my own term (thinking a step above first principles, with first principle-base set)
  see mathematical creativity below
contrast with David Wees' review  http://davidwees.com/content/evaluating-mathematical-thinking-mooc
both calculation and understanding are important
education ≠ solely acquisition of specific tools to use in a subsequent career  
  culture, life ≠ job
  education focus must be on learning how to learn
With complexity, paradoxes and unknown implications develop
  mathematics is understood only through mathematics  
  not verifiable by other means
  methods explain subject
math = carrier of conceptual properties
  Dirichlet: function = any rule that produces new (numbers) objects from old
    behaviour > formula  
    injectivity = unique inputs produce unique outputs
  Riemann: complex function = property of differentiability  
  real analysis (continuity, differentiability)
  Gauss: residual classes
  sets (behaviours specified by axioms)
  Dedekind: ring, field, ideal = collection of objects endowed with certain operations

Two mathematical skills
1. Mathematically Able  
   given a mathematical problem, find its mathematical solution
2. Mathematically Creative  
   given a problem, describe key features mathematically, then find its mathematical solution
   conceptually understand, learn quickly, see things in new ways, acquire new techniques, adapt old for new,
   know when/how apply, power, scope, limitations, skills, cross-disciplinary, teamwork

Formal notations
  patterns are abstract in nature  
  notation is abstract  
  formalize for communication
  spoken languages are cumbersome and ambiguous  
  math language for efficiency and accuracy (disambiguate)

Scope of course
  Goal. develop mathematical creativity and thinking skills  
  http://livebinders.com/play/play_or_edit?id=121248
  Content. logic, formal notation, proof, number theory, real analysis
Lesson 1 - Introductory Material

What is mathematics?
- science of patterns
- precise language
- literal vs inferred meanings

Math must use literal meanings (like science) for unambiguous communication
to determine, must know what statement says/means precisely
words and language are ambiguous (eg. dangling modifiers)
typically interpret via context (eg. Is August always in Summer? What does 'in' mean?)

Forms of precision
1. Definition of Object: object a has property p
2. Definition of Type: every object of type T has property p
3. Statement of Existence: there is an object of type T having property p (ambiguous: of object only? Of type?)
4. Statement of Implication: if statement , then statement b

Formal logic
- And/Or/Not combinators
- For All/There Exists modifiers

Ways of proving
eg. N = (p₁ × p₂ × p₃ × ... × pₙ) + 1

Lesson 2 - Analysis of Language (Logical Combinators)

And ($\land$)
$\phi \land \psi$ means both $\phi$ and $\psi$ are true  
$\phi$ and $\psi$ are conjugates of conjunction $\phi \land \psi$
($\pi > 3$) \land ($\pi < 3.2$) = $3 < \pi < 3.2$

And is commutative, associative, and distributive across a disjunction

Or ($\lor$)
$\phi \lor \psi$ means either $\phi$ or $\psi$ (or both) are true  
$\phi$ and $\psi$ are disjuncts of disjunction $\phi \lor \psi$
the word 'or' is ambiguous
- inclusive 'or': $a \cdot b = 0$ if $a = 0$ or $b = 0$ (at least one of $a = 0$ or $b = 0$ must be true for $ab = 0$ to be true)
- either or both (at least one) are possible
- exclusive 'or': $a > 0$ or $x^2 + a = 0$ has a real root (only one of $a > 0$ and $x^2 + a = 0$ is possible or true)
in mathematics, 'or' is inclusive by default

Or is commutative, associative, and distributive across a conjunction

Not ($\neg$)
Not negates the object or statement that follows (it turns true false and false true)
$\neg(\pi < 3) = \pi \not< 3 = \pi \geq 3$  
$\geq$ not $>$
if $\psi$ is true, then $\neg\psi$ is false  
if $\psi$ is false, then $\neg\psi$ is true

<table>
<thead>
<tr>
<th>$\phi$</th>
<th>$\neg\phi$</th>
<th>$\psi$</th>
<th>$\neg\psi$</th>
<th>$\phi \land \psi$</th>
<th>$\phi \lor \psi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Truth Table
Negated must belong to same population as unnegated.

All foreign cars are badly made. (F)
Possible negations (first four good candidates, since same population; last one bad candidate, since diff population):
All foreign cars are well made. (F)
All foreign cars are not badly made. (F)
At least one foreign car is well made. (F)
At least one foreign car is not badly made. (T) best negation
All domestic cars are well made. (F) bad candidate

Lesson 3 – Analysis of Language (Logical Implication)

Condition or Implication (⇒)

ϕ ⇒ ψ means ϕ implies ψ  
ϕ is the antecedent and ψ is the consequent of the implication ϕ ⇒ ψ
implication is noncommutative we assume the antecedent (if), we deduce the consequent (then)
this means implication = condition + causality
define the truth of ϕ ⇒ ψ in terms of the truth or falsity of ϕ and ψ  this way, the condition is always defined
conditional: the truth of ψ follows the truth of ϕ
causation: ψ follows ϕ (we ignore this in this course)

Conditional Truth Table

<table>
<thead>
<tr>
<th>ϕ</th>
<th>ψ</th>
<th>ϕ ⇒ ψ</th>
<th>¬ϕ</th>
<th>¬ϕ ⇒ ¬ψ</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>¬F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>?₁</td>
<td>¬F</td>
<td>¬F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>?₂</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>?₃</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

assume ϕ, N > 7 (T), deduce ψ, N² > 40 (T). ϕ ⇒ ψ is T (conditionally and causally)

contradiction. if ?₁ = T, the truth of ψ follows from the truth of ϕ, but ψ is false . . . ?₁ = F
reverse argument. cannot have ϕ T and ψ F if ϕ ⇒ ψ T, so if ϕ T and ψ F, ϕ ⇒ ψ F
(no condition nor causality)

negate ϕ and ψ, ϕ F ⇒ ψ T, ψ F ⇒ ψ F, ψ F ⇒ ψ T
then calculate ¬ϕ ⇒ ¬ψ, ¬ϕ F ⇒ ¬ψ F, ¬ϕ T ⇒ ¬ψ T
 negate ¬ϕ ⇒ ¬ψ so ϕ ⇒ ψ : ¬ϕ ⇒ ¬ψ F, ϕ ⇒ ψ T, ¬ϕ ⇒ ¬ψ T, ¬ϕ ⇒ ¬ψ F
however, if ϕ and ψ are both false, ϕ ⇒ ψ is true

Conclusion: ϕ does not imply ψ if, even though ϕ is true, ψ is nevertheless false
in all other circumstances, ϕ ⇒ ψ is T

Example. Given ϕ : √2 is irrational, and ψ : 0 < 1  Is ϕ ⇒ ψ true? No, both true, but ϕ does not cause ψ (no causality)
ϕ ⇒ ψ is equivalent to (ϕ ∧ ψ) ∨ (¬ϕ)

<table>
<thead>
<tr>
<th>ϕ</th>
<th>ψ</th>
<th>ϕ ∧ ψ</th>
<th>¬ϕ</th>
<th>(ϕ ∧ ψ) ∨ (¬ϕ)</th>
<th>ϕ ⇒ ψ</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Conclusion: ϕ does not imply ψ if, even though ϕ is true, ψ is nevertheless false

in all other circumstances, ϕ ⇒ ψ is T

Example. Given ϕ : √2 is irrational, and ψ : 0 < 1  Is ϕ ⇒ ψ true? No, both true, but ϕ does not cause ψ (no causality)
ϕ ⇒ ψ is equivalent to (ϕ ∧ ψ) ∨ (¬ϕ)

<table>
<thead>
<tr>
<th>ϕ</th>
<th>ψ</th>
<th>¬ϕ</th>
<th>(ϕ ∧ ψ) ∨ (¬ϕ)</th>
<th>ϕ ⇒ ψ</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
Lesson 4 – Analysis of Language (Logical Equivalence)

**Bicondition or Equivalence (↔)**

φ ↔ ψ means φ implies ψ and ψ implies φ  
φ and ψ are **logically equivalent** if each implies the other

abbreviation of (φ ⇒ ψ) ∧ (ψ ⇒ φ)

conjunction of φ ⇒ ψ and ψ ⇒ φ truth tables

<table>
<thead>
<tr>
<th>φ</th>
<th>ψ</th>
<th>φ ⇒ ψ</th>
<th>(φ ⇒ ψ) ∧ (ψ ⇒ φ)</th>
<th>φ ↔ ψ</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

φ ↔ ψ is true if φ and ψ are both true or both false

φ ⇒ mathematically means implies, φ ↔ ψ and ↔ ψ mean equivalence (↔ ψ is ambiguous, also means back implies)

The following mean φ and ψ are equivalent.

1. φ is necessary and sufficient for ψ
2. φ if and only if ψ

Which of the following conditions is necessary for “the natural number n to be a multiple of 10”?

Ask: Does n being a multiple of 10 imply the conditions?

Which of the following conditions is sufficient for “the natural number n to be a multiple of 10”?

Ask: Is n being a multiple of 10 implied by the conditions? Do the conditions imply n is a multiple of 10?

Which of the following conditions is necessary and sufficient for “the natural number n to be a multiple of 10”?

Combine answers to first two questions.
Lesson 5 – Analysis of Language (Logical Quantifiers)

There exists, There is or Is (∃)

∃x means at least one x exists ∃ is an existential quantifier

There is an object x having property p.

The equation $x^2 + 2x + 1 = 0$ has a real root.

There is a real number x such that $x^2 + 2x + 1 = 0$.

$\exists x \ [x^2 + 2x + 1 = 0]$ means $\exists x$ binds $x^2 + 2x + 1 = 0$

prove by finding an actual x that solves the equation

proof: let $x = -1$, then $x^2 + 2x + 1 - 2 + 1 = 0$

$\exists x \ [x^3 + 3x + 1 - 0]$ y - $x^3 + 3x + 1$ is a continuous function.

if $x = -1$, this curve has value $y = -1 - 3 + 1 = -3$ (below y axis)
if $x = 1$, this curve has value $y = 1 + 3 + 1 = 5$ (above y axis)

indirect proof – found there is an x that solves, not what value of x solves

wobby table theorem – rotate table until stable (trial and error)

is x negative or positive? (curve b or a on graph)

for b, $(\exists x < 0) \ [x^3 + 3x + 1 - 0]$ for a, $(\exists x > 0) \ [x^3 + 3x + 1 - 0]$

what if $x = 0$? $y = 0 + 0 + 1 - 1 = -1$ (below y axis)

or we could simply observe that $x \geq 0$, then $x^3 + 3x + 1 > 0 \ (x \neq 0)$

so b is false, which means a is true

$\sqrt{2}$ is rational.

There exist natural numbers p and q such that $\sqrt{2} = p/q$.

$\exists p \exists q \ [\sqrt{2} - p/q]$

make it more specific by writing $(\exists p \in \mathbb{N})(\exists q \in \mathbb{N}) \ [\sqrt{2} - p/q]$, where $\mathbb{N}$ – the set of all natural numbers

avoid $(\exists p, q \in \mathbb{N}) \ [\sqrt{2} - p/q]$ ambiguous p – any real number p or any natural number p

q – any natural number q

prove that $\sqrt{2}$ is not rational

$\neg(\exists p \in \mathbb{N})(\exists q \in \mathbb{N}) \ [2 - p^2/q^2]$

Any or For all (∀)

∀x means for all x ∀ is a universal quantifier

For any x, the property p applies.

The square of any real number is greater than or equal to zero.

$(\forall x \in \mathbb{R}) \ [x^2 \geq 0]$

this is different from $(\exists x \in \mathbb{R}) \ [x^2 \geq 0]$ - There is a real number whose square is greater than or equal to zero.
Lesson 6 - Working with Quantifiers

Negating Statements that have Quantifiers

Let x - motorist, A(x) - run red lights
Show that \( \neg[\forall x A(x)] \iff \exists x \neg A(x) \)
so \( \neg \forall \iff \exists \) and \( \neg \exists \iff \forall \)

Familiar: "It is not true that all motorists run red lights." \( \iff " \)There is a motorist that does not run red lights."

Abstraction.
\( \Rightarrow \) assume \( \neg[\forall x A(x)] \)
If it is not the case that for all x, A(x), then at least one x must fail to satisfy A(x). So, for at least one x, \( \neg A(x) \)
is true. In symbols, \( \exists x \neg A(x) \).
\( \Leftarrow \) assume \( \exists x \neg A(x) \)
If there is an x for which A(x) is false, then A(x) cannot be true for all x. In other words, \( \forall x A(x) \) must be false. In symbols, \( \neg[\forall x A(x)] \).

All domestic cars are badly made.
Let C - (population of) all cars, D(x) - domestic, M(x) - badly made
\( \forall x \in C \) \( D(x) \Rightarrow M(x) \)
We know \( D(x) \neq M(x) \) \( \iff D(x) \land \neg M(x) \)
\( \neg(\forall x \in C) \) \( D(x) \Rightarrow M(x) \) \( \iff (\exists x \in C) \) \( \neg[D(x) \Rightarrow M(x)] \) \( \iff (\exists x \in C) \) \( D(x) \neq M(x) \) \( \iff (\exists x \in C) \) \( D(x) \land \neg M(x) \)
There is a domestic car that is not badly made.

why not \( (\exists x \neq C) \) ? population - C do not change population (domain of quantification)

All prime numbers are odd.
Let P(x) - x is prime, O(x) - x is odd
\( \forall x \) \( P(x) \Rightarrow O(x) \)
\( \neg \forall x \) \( P(x) \Rightarrow O(x) \) \( \iff \exists x \) \( P(x) \neq O(x) \) \( \iff \exists x \) \( P(x) \land \neg O(x) \)
There is a prime number that is not odd.

All prime numbers bigger than 2 are odd.
Let P(x) - x is prime, O(x) - x is odd
\( \forall x \geq 2 \) \( P(x) \Rightarrow O(x) \)
\( \neg(\forall x) \geq 2 \) \( P(x) \Rightarrow O(x) \) \( \iff (\exists x \geq 2) \) \( P(x) \neq O(x) \) \( \iff (\exists x \geq 2) \) \( P(x) \land \neg O(x) \)
There is a prime number bigger than 2 that is not odd.

There is an unhealthy player on team T.
Let x - person, P(x) - x plays for team T, H(x) - x is healthy
\( \exists x \) \( P(x) \land \neg H(x) \)
\( \neg \exists x \) \( P(x) \land \neg H(x) \) \( \iff \forall x \) \( \neg[P(x) \lor H(x)] \) \( \iff \forall x \) \( \neg[P(x) \lor H(x)] \)
All players on team T are healthy. (do not do this)

Combining Quantifiers order is important

There is no largest natural number.
\( \forall m \in \mathbb{N} \) \( \exists n \in \mathbb{N} \) \( m < n \) true

There is a natural number bigger than all natural numbers.
\( \exists n \in \mathbb{N} \) \( \forall m \in \mathbb{N} \) \( m < n \) false

One American dies every hour.
\( \exists A \forall H \) \[A \text{ dies in hour } H\] literal, false

Every hour an American dies.
\( \forall H \exists A \) \[A \text{ dies in hour } H\] meant, true

Do you have a licence from more than one state?
literal - same licence comes from (issued by) more than one state
\( \exists(S_1) \) \( \exists(S_2) \) \[S_1 \neq S_2 \land \text{From}(L,S_1) \land \text{From}(L,S_2)\] literal, false (truth. each licence is issued by only one state)

\( \exists(S_1) \) \( \exists(S_2) \) \[L_1 \neq L_2 \land \text{From}(L_1,S_1) \land \text{From}(L_2,S_2)\] not meant (two licences from one state), possibly true

\( \exists(S_1) \) \( \exists(S_2) \) \( \exists(S_3) \) \[L_1 \neq L_2 \land (S_1 \neq S_2) \land \text{From}(L_1,S_1) \land \text{From}(L_2,S_2)\] meant, true

A driver's licence valid in one state is valid in any state.
\( \forall L \) \( \exists(S) \) \[\text{Valid}(L,S) \Rightarrow \forall S \exists(S) \text{Valid}(L,S)\] meant, true (for any licence, if the licence is valid in a state, then (implies) the licence is valid in all states)

\( \exists(S) \) \( \exists(S_2) \) \[S_1 \neq S_2 \land \text{Valid}(L_1,S_1) \land \text{Valid}(L_2,S_2)\] irrelevant, true (a licence is valid in two states)

\( \forall L \) \( \exists(S) \) \[\forall S \exists(S) \text{Valid}(L,S) \lor \forall S \exists(S) \text{Valid}(L,S)\] every licence is valid in every pair of states, false (some invalid)
Combining Quantifiers with Conjunctions and Disjunctions

let \(E(x)\) - \(x\) is even, \(O(x)\) - \(x\) is odd

\[
\begin{align*}
\forall x \ [E(x) \lor O(x)] & \quad \text{all natural } x \text{ are either even or odd} \quad T \\
\forall x E(x) \lor \forall x O(x) & \quad \text{all natural } x \text{ are even or all natural } x \text{ are odd} \quad F \\
\exists x \ [E(x) \land O(x)] & \quad \text{some natural } x \text{ are even and odd} \quad F \\
\exists x E(x) \land \exists x O(x) & \quad \text{some natural } x \text{ are even and some natural } x \text{ are odd} \quad T
\end{align*}
\]

Domain of Quantification (population) - What does \(x\) denote?

quantifier only tells you something if you know what \(x\) denotes

\[
\begin{align*}
\forall x \ [x > 0 \Rightarrow \exists y(xy = 1)] & \quad T \text{ or } F? \\
\text{if } x \text{ - natural number} & \quad (\forall x \in \mathbb{N}) \ [x > 0 \Rightarrow (\exists y \in \mathbb{N}) (xy - 1)] \quad \text{makes sense, } F \\
\text{if } x \text{ - rational number} & \quad (\forall x \in \mathbb{Q}) \ [x > 0 \Rightarrow (\exists y \in \mathbb{Q}) (xy - 1)] \quad \text{makes sense, } T \\
\text{if } x \text{ - baseball player} & \quad (\forall x \in B) \ [x > 0 \Rightarrow (\exists y \in B) (xy - 1)] \quad \text{does not make sense}
\end{align*}
\]

nested domains of quantification (multiple populations)

let \(x, y, z\) - real numbers (\(\mathbb{R}\))

\(\exists x \in \mathbb{Q}\) (rational), \(\exists y \in \mathbb{Z}\) (integer), \(\exists z \in \mathbb{N}\) (natural)

let \(A\) - set of animals, \(S(x)\) - has spots:

\(L\) - set of leopards

\(T\) - set of tigers

\(H\) - set of horses

\[
\begin{align*}
\forall x \in L)S(x) & \quad (\forall x \in A) [L(x) \Rightarrow S(x)] \quad \text{Every leopard has spots.} \\
\forall x \in T)\neg S(x) & \quad (\forall x \in A) [T(x) \Rightarrow S(x)] \quad \text{No tiger has spots.} \\
\exists x \in H)S(x) & \quad (\exists x \in A) [H(x) \Rightarrow S(x)] \quad \text{Some horses have spots.}
\end{align*}
\]

Implicit Quantification

mathematicians sometimes omit quantifiers please avoid omitting quantifiers

\(x \geq 0 \Rightarrow \sqrt{x} \geq 0\) means \(\forall x \in \mathbb{R}) \ [x \geq 0 \Rightarrow \sqrt{x} \geq 0]\)

Lesson 7 - Arguments and Proofs

Theorem - statement want to prove (well established by study and proof)

Lemma - proposal of truth (little theorem)

Argument - point made in a proof

Proof - solution which logically confirms or refutes a theorem

Why use proofs? establish truth (theorem sound), communicate to others (explanation/justification of why true)

no particular layout or format no templates

about logical structure (thought sculpture)

every step counts, has a result, steps understandable - elegant (aesthetics)

Where start proofs? if proof starts in \(\phi\), it must culminate in \(\phi\)

proof by reverse argument, argue successfully backward from \(\phi\) many possible starts, one goal converging

proof by contradiction, argue successfully forward from \(\neg \phi\) one start, many possible goals diverging

use proof by contradiction to:

prove non-existence statement

start proving when no obvious start
How prove? about logical structure (thought sculpture)
unpack to useful information reason with concepts
analyze statements reason ways to test
include. theorem (start), systematic argument, result (conclusion)
systematic argument. every step counts, steps understandable, argument thorough yet concise
use formal language for clear communication
elegant = theorem + systematic argument + result + formal language aesthetic

Example. Proof by contradiction

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>want to prove statement $\phi$</td>
<td>start</td>
</tr>
<tr>
<td>2.</td>
<td>start by assuming $\neg \phi$ theorem</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>reason until reach a (any) conclusion that is false</td>
<td>systematic argument</td>
</tr>
<tr>
<td>4.</td>
<td>true assumption cannot lead to false conclusion</td>
<td>system</td>
</tr>
<tr>
<td>5.</td>
<td>assumption (theorem) $\neg \phi$ must be false</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>in other words, statement $\phi$ must be true</td>
<td>conclusion</td>
</tr>
</tbody>
</table>

$\sqrt{2}$ is irrational

Statement. $\sqrt{2}$ is irrational

Proof.
contradiction. assume, on the contrary, that $\sqrt{2}$ were rational (theorem)
systematic reasoning,
let p and q be natural coprimes, such that $\sqrt{2} = p/q$, where p/q is in simplest terms (no common factors)
rearrange. $p = \sqrt{2} q$
square. $p^2 = 2q^2$
interpret. so, since the square of an even number is even and the square of an odd number is odd,
$E \times E = (2n)(2n) = 4n^2 = 2(2n^2)$ even
$O \times O = (2n+1)(2n+1) = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$ odd
$p^2$ is even and $p$ is even
redefine. so. $p = 2r$ for some natural number $r$
rearrange, substitute for $p$ and simplify. $2q^2 - p^2 - (2r)^2 - 4r^2$, $2q^2 - 4r^2$, $q^2 - 2r^2$
interpret. so, $q^2$ is even and $q$ is even, as above for $p^2$
interpret. so, $p$ and $q$ are both even (both have a factor of 2)
contradiction. but this is impossible since $p$ and $q$ are coprimes (have no common factors)
interpret. therefore, began with a false assumption
interpret. so, theorem is false

Conclusion. if assumption (theorem) is false, statement is true, $\sqrt{2}$ must be irrational QED

Truth-table Analysis of Proof of Contradiction (using $\phi \Rightarrow \psi$)
carry out proof that $\phi \Rightarrow \psi$ is true (truth table)
accept when $\psi$ and $\phi \Rightarrow \psi$ true, reject when $\phi \Rightarrow \psi$ false (proof false)
if $\phi \Rightarrow \psi$ true and $\psi$ false (contradiction), $\phi$ is false (false assumption)

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\phi$</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>$\psi$</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>$\phi \Rightarrow \psi$</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
Proving Conditionals

given $\phi \Rightarrow \psi$
we know $\phi \Rightarrow \psi$ is true if $\phi$ is false, so to test truthfulness of $\phi \Rightarrow \psi$ we can assume $\phi$ is true (see truth table above)
to prove it, we assume $\phi$ and deduce $\psi$

examples.

let $x$ and $y$ be variables for real numbers
prove that "$x$ and $y$ are rational" implies that "$x+y$ is rational"

start: assume $x$ and $y$ are rational
argue: then there are integers $p$, $q$, $m$, and $n$ such that $x = p/m$ and $y = q/n$
then $x+y = p/m + q/n = (pn+qm)/(mn)$, which is rational
conclude: hence $x+y$ is rational

let $r$ and $s$ be irrational numbers
which of the following are necessarily irrational
$r+3$ so irrational
$r-s$ so irrational
$\sqrt{r}$ so irrational

Proving Conditionals involving Quantifiers

sometimes best handled by proving the contrapositive
to prove $\phi \Rightarrow \psi$, prove $(\neg \phi) \Rightarrow (\neg \psi)$

prove $(\sin \theta \neq 0) \Rightarrow (\forall n \in \mathbb{N}) [\theta \neq n\pi]$

$\neg (\sin \theta \neq 0) \Rightarrow (\forall n \in \mathbb{N}) [\theta \neq n\pi] \Leftrightarrow \neg (\forall n \in \mathbb{N}) [\theta = n\pi] \Rightarrow (\sin \theta = 0) \Leftrightarrow (\exists n \in \mathbb{N}) [\theta = n\pi]$

we know this is true ($n = 2m\pi, m \in \mathbb{N}$)
this proves the desired result

Proving Biconditionals

given $\phi \iff \psi$
we generate two proofs, one of $\phi \Rightarrow \psi$, the other of $\psi \Rightarrow \phi$
sometimes best handled by proving $\phi \Rightarrow \psi$ and $(\neg \phi) \Rightarrow (\neg \psi)$, where $(\neg \phi) \Rightarrow (\neg \psi)$ is the contrapositive of $\psi \Rightarrow \phi$

Lesson 8 – Methods of Proof

Methods of Indirect Proof

prove $\exists x A(x)$
official way is to find an object $a$ for which $A(a)$
method of specific example

show some number is irrational by proving $\sqrt{2}$ is irrational
this does not always work

theorem. there are irrationals $r$ and $s$ such that $r^s$ is rational

proof. by method of proof–by–cases (two cases)

1. if $((\sqrt{2})^{1/2})^{1/2}$ is rational, take $r = s - \sqrt{2}$
rational

2. if $((\sqrt{2})^{1/2})^{1/2}$ is irrational, take $r = (\sqrt{2})^{1/2}$ and $s = \sqrt{2}$
then $r^s = ((\sqrt{2})^{1/2})^{1/2} - (\sqrt{2})^{1/2} - (\sqrt{2})^2 - 2$
rational

conclusion. theorem is proved (there are irrationals $r$ and $s$ such that $r^s$ is rational)
theorem: \( \forall n \exists m (m > n^2) \)

proof: by arbitrary number

take arbitrary \( x \) and show that it satisfies \( A(x) \)

warning. What is arbitrary? How is it picked?

pick arbitrary ≠ pick in arbitrary way

pick arbitrary = generalized variable, know nothing about object \( \therefore \) any \( \therefore \) all

\( \therefore \) can “ignore” specificity since any case works, so show a case works

pick in arbitrary way = specific object once choice made (sampling error/bias)

let \( n \) = arbitrary natural number

\( \therefore \) unspecified variable (not a constant, open value)

set \( m = n^2 + 1 \)

then \( m > n^2 \)

demonstrates \( \exists m (m > n^2) \)

it follows that \( \forall n \exists m (m > n^2) \)

demonstrates because \( n \) is arbitrary (could be any \( n \))

Method of Contradiction

prove \( \forall x A(x) \) assume \( \neg \forall x A(x) \equiv \exists x \neg A(x) \)

theorem: \( \forall x A(x) \)

proof: by contradiction

\( \neg \forall x A(x) \equiv \exists x \neg A(x) \)

let \( c \) be an object such that \( \neg A(c) \)

now reason with \( c \), and fact that \( \neg A(c) \), to derive contradiction(s)

Method of Induction

prove \( \forall n A(n) \)

establish following two statements

1. \( A(1) \) works/is true \hspace{1cm} \text{initial case, initial step, first step}
2. \( (\forall n) [A(n) \Rightarrow A(n+1)] \) \hspace{1cm} \text{induction step}

intuitively, this gives \( \forall n A(n) \) as follows

by step 1, \( A(1) \)

by step 2, \( A(1) \Rightarrow A(2) \), \( A(2) \Rightarrow A(3) \), \( A(3) \Rightarrow A(4) \), \( \ldots \), \( A(n) \Rightarrow A(n+1) \)

check first few cases \hspace{1cm} \text{pattern} \hspace{1cm} \text{capitalize on pattern to induce (identify “rule” of pattern)}

prove \( 1 + 2 + \ldots + n = (1/2)(n)(n+1) \) over \( \mathbb{N} \)

beware logic leaps and jumping to conclusions

\[
\begin{align*}
 n - 1 & : 1 & (1/2)(1)(1+1) - (1/2)(1)(2) = 1 \\
 n - 2 & : 1 + 2 = 3 & (1/2)(2)(2+1) - (1/2)(2)(3) = 3 \\
 n - 3 & : 1 + 2 + 3 = 6 & (1/2)(3)(3+1) - (1/2)(3)(4) = 6 \\
 n - 4 & : 1 + 2 + 3 + 4 = 10 & (1/2)(4)(4+1) - (1/2)(4)(5) = 10 \\
\ldots
\end{align*}
\]

prove \( P(n) = n^2 + n + 41 \) \hspace{1cm} Euler 1772

pattern: all values of \( P(n) \) for \( n = 1, 2, \ldots \), etc. are prime numbers \hspace{1cm} until reach \( n=41 \)

but \( P(41) = 1681 = 41^2 \) \hspace{1cm} pattern is apparent only (not actually true)
we need an axiom or principle to make the method of induction work

this PMI is what tells us that steps 1 and 2 (above) yield \( \forall n A(n) \)

equation - solve for \( n \)

identity - states expressions are equal

theorem: for any natural number \( n \), \( 1+2+3+\ldots+n = \frac{(1/2)(n)(n+1)}{2} \)

proof: by mathematical induction

step 1. for \( n = 1 \), identity \( 1+2+3+\ldots+n = \frac{(1/2)(n)(n+1)}{2} \) reduces to

\( \frac{(1/2)(1)(1+1)}{2} = \frac{(1/2)(1)(2)}{2} \) true (both sides equal 1)

step 2. induction

assume identity holds for \( n \) \n
want to deduce identity for \( n + 1 \)

how? try adding \( n + 1 \) to both sides of *, see if get **

\( 1+2+3+\ldots+n+(n+1) = \frac{(1/2)(n)(n+1)}{2}+(n+1) \)

(\( (1/2)(n)(n+1)+(1/2)(2)(n+1) \)

(\( (1/2)(n)2 + 2(n+1) \)

(\( (1/2)(n^2 + 3n + 2) \)

(\( (1/2)(n+1)(n+2) \)

(\( (1/2)(n+1)(n+1+1) \)

\( 1+2+3+\ldots+n+(n+1) = \frac{(1/2)(n)(n+1)}{2}+(n+1) \) which is ** which is the identity * with \( n + 1 \) in place of \( n \)

conclude: by the PMI, the identity holds for all \( n \)

theorem: if \( x > 0 \), then for any natural number \( n \), \( (1+x)^{n+1} > 1+(n+1)x \)

proof: by mathematical induction

let \( A(n) \) be the statement \( (1+x)^{n+1} > 1+(n+1)x \) for \( \forall n A(n) \)

step 1. \( A(n) = (1+x)^{n+1} > 1+(n+1)x \)

by binomial theorem, \( (1+x)^2 = 1+2x+x^2 \) so \( 1+2x+x^2 > 1+2x \) (since \( x^2 > 0 \) when \( x > 0 \)) so true

step 2. \( \forall n \ [A(n) \Rightarrow A(n+1)] \)

pick an arbitrary \( n \) and prove \( A(n) \Rightarrow A(n+1) \)

we assume \( A(n) = (1+x)^{n+1} > 1+(n+1)x \)

we deduce \( A(n+1) = (1+x)^{n+2} > 1+(n+2)x \)

\( (1+x)^{n+2} - (1+x)(1+x)^{n+1} \)

.: try \( (1+x)^* \), see if get **

\( \frac{(1+x)(1+n+1)x}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^2]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^3]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^4]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^5]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^6]}{2} \)

\( \frac{(1+n+1)x + x[1+(n+1)x^7]}{2} \)

\( 1+(n+2)x+(n+1)x^2 \) (since \( x^2 > 0 \) when \( x > 0 \))

so, \( (1+x)(1+x)^{n+1} > 1+(n+1)x+(n+1)x^2 \) (since \( x^2 > 0 \) when \( x > 0 \))

\( 1+(n+2)x+(n+1)x^2 \) \( (1+x)^{n+1} > 1+(n+2)x \) \( (1+x)^{n+2} > 1+(n+2)x \)

\( (1-x)^{n+2} > 1+(n+2)x \) is **

conclude: by the PMI, the identity holds for all \( n \)
Summary of Proof by Induction Method
1. want to prove that some statement \( A(n) \) is valid for all natural numbers \( n \) (\( \forall n \in \mathbb{N} \))
2. first, prove \( A(1) \), usually a matter of simple observation often easy trips people up (watch out)
3. second, give an algebraic argument to establish the conditional \( A(n) \Rightarrow A(n+1) \)
4. reduce \( A(n+1) \) to a form where we can use \( A(n) \) to deduce it
5. conclude, by PMI (say this = heavy weight), this proves \( \forall n A(n) \) (infinite collection, subtleties, complexities)

need both 2 and 3

Common Variant of Induction
\( A(1) \) may not be true need to prove a statement of the form (\( \forall n \geq n_0 \))\( A(n) \)
1. verify \( A(n_0) \)
2. prove (\( \forall n \geq n_0 \)) \( [A(n) \Rightarrow A(n+1)] \)

example: The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic

theorem: every natural number greater than 1 is either prime or a product of primes

not true at \( n = 1 \) (only natural \( n \) where theorem is not true) cannot use default PMI to prove, must use variant

\( A(n) \): \( \forall m \ [2 \leq m \leq n] \Rightarrow m \) is either a prime or a product of primes

proof: by mathematical induction (\( A(n) \) variant)

step 1: \( A(2) \): \( m = 2 \) (2 is either prime or a product of primes)

2 is prime so true

step 2: \( \forall n \ [A(n) \Rightarrow A(n+1)] \)

let \( m \) - a natural number such that \( 2 \leq m \leq n+1 \)

if \( m \leq n \), then by \( A(n) \), \( m \) is either prime or a product of primes

cases.

case 1: if \( m = n+1 \), then \( m \) is prime

case 2: if \( m = n+1 \) and if \( n+1 \) is not prime, then there must be natural numbers \( p \) and \( q \) such that

\( 1 < (p, q) < n+1 \) and \( n+1 = pq \)

since \( 2 \leq (p, q) \leq n \), by \( A(n) \), \( p \) and \( q \) are either prime or products of primes

hence, since \( n+1 = pq \), \( n+1 \) is a product of primes

so, since \( m = n+1 \), \( m \) is a product of primes

so, true

conclusion: the theorem follows by induction

downward proof: prove statement with lesser numbers

Lesson 9 - Elements of Set Theory

Set - well-defined collection of objects

define by specifying collection, unless arbitrary collection \( A \) - set, \( x \in A \) element or member of set

\( (x \in \mathbb{Q}) \land (x > 0) \) means \( x \) is a positive rational number

specifying set

list elements \( \{\ldots, n\} \{\ldots, n, n\ldots\} \{\ldots, n\ldots\} \)

define set property \( \{x \mid A(x)\} \{x \in X \mid A(x)\} \)
Examples of Sets

\[ \mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}\]
\[ \mathbb{Q} = \{x \in \mathbb{Q} \mid (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z}) \ [(m > 0) \land (mx - n)]\}\]
\[ \{\sqrt{2}, -\sqrt{2}\} = \{x \in \mathbb{R} \mid x^2 = 2\}\]
\[ \{1, 2, 3\} = \{x \in \mathbb{N} \mid x < 4\}\]

Empty or Null Set (\(\emptyset\))

\(\emptyset - \text{oslash (Scandinavian oeu)}\)

\[ \emptyset = \{x \in \mathbb{R} \mid x^2 < 0\}\]
\[ \emptyset = \{x \in \mathbb{N} \mid 1 < x < 2\}\]
\[ \emptyset \neq \{\emptyset\}\]
\[ \emptyset - \text{no members}\]
\[ \{\emptyset\} - \text{one member} \emptyset \in \{\emptyset\}\]

Set Properties

property extensions

\[ \mathbb{Q} = \{m/n \mid \exists m \in \mathbb{Z}, \exists n \in \mathbb{Z}, n \neq 0\}\]

equal sets

A - B if A and B have exactly the same elements
equality of sets does not mean they have identical definitions

any set can have many definitions
to prove A - B, split proof into two parts
1. show that every member of A is a member of B
2. show that every member of B is a member of A

arbitrary element

(\(\forall x \in A\) [x \in B])

(\(\forall x \in B\) [x \in A])
similar to equivalence (bicondition)

subsets

let A = \{1, 2\}, B = \{1, 2, 3\}

A \subseteq B\ every element of A is a member of B

A \subset B\ proper subset, emphasize A and B unequal

A - B iff (A \subseteq B) \land (B \subseteq A)

Set Operations

union + addition

A \cup B\ set of all objects in A plus set of all objects in B (members in either A and B)

A \cup B = \{x \mid (x \in A) \lor (x \in B)\}\]

intersection \times multiplication

A \cap B\ set of all objects which A and B have in common (members in both A and B)

A \cap B = \{x \mid (x \in A) \land (x \in B)\}\]

disjoint - there are no objects in common

A \cap B = \emptyset\]

complement \neg negation

A'\ set of all elements of U not in A (members not in A)

A' = \{x \in U \mid x \notin A\}\]

U - universal set\ set of all objects of the kind being considered (population of objects with same properties)

when dealing with sets, usually sets of objects have the same considered properties (are of the same kind)
Set-operation Properties

let A, B and C be subsets of U

1. \( A \cup (B \cup C) = (A \cup B) \cup C \)
   associative property of union

2. \( A \cap (B \cap C) = (A \cap B) \cap C \)
   associative property of intersection

3. \( A \cup B = B \cup A \)
   commutative property of union

4. \( A \cap B = B \cap A \)
   commutative property of intersection

5. \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \)
   distribution of union across intersection

6. \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \)
   distribution of intersection across union

7. \( (A \cup B)' = A' \cap B' \)
   negation of union (De Morgan Law 1)

8. \( (A \cap B)' = A' \cup B' \)
   negation of intersection (De Morgan Law 2)

9. \( A \cap A' = U \)
   complement of union (Complementation Law 1)

10. \( A \cup A' = \emptyset \)
    complement of intersection (Complementation Law 2)

11. \( (A')' = A \)
    Self-inverse Law

Key to the Set-operation Properties Venn Diagrams

the Venn diagrams on the previous page correspond to the set-operation properties on this page

fill - illustration of property, yellow - filled first, orange - filled second or full property, white - not filled (empty)

diagrams 1, 3, 7, 8, 9: all coloured areas illustrate the property, the yellow area(s) show the first step

diagrams 2, 5, 6: only orange area illustrates the property, the yellow area(s) show the first step

diagrams 7, 8: A' = B' (no real border between colours, coloured as is to "show" steps), should be one colour

diagrams 7, 8, 9, 10, 11: A' and A' = B' are infinite in spread (bordered here to contain fill)

Lesson 10 – Elements of Number Theory

natural numbers arithmetic total, product, difference integer results (trivial)

quotient, remainder real results (so division is where the action is)

Division Theorem rigorous proofs – method important, not result

if a and b are integers and b > 0, then there are unique integers q and r such that a = qb + r and 0 ≤ r ≤ b

two parts to proof: proof of existence (there are) and proof of uniqueness (unique)

proof of existence

look at the non-negative integers of the form a – kb, where k is an arbitrary integer, and show that one of the non-negative integers is less than b

do such integers exist?

\[ k = -\lfloor a \rfloor \]

then, since \( b ≥ 1 \) (it is non-negative and > 0 by definition above), \( a - kb = a + |a|b \)

if \( b = 1 \), \( a + |a| ≥ 0 \)

let \( r \) be the smallest such integer and let \( q \) be the value of \( k \) for which \( r \) occurs

\[ r = a - qb \]

there are \( r \) and \( b \)

to complete the proof, we show that \( r < b \) suppose, instead, that \( r ≥ b \), then \( 0 ≤ r - b = a - qb - b = a - (q + 1)b \)

thus \( a - (q + 1)b \) is a non-negative integer of the form \( a - kb \), of which \( r \) is the smallest such,

yet \( a - (q + 1)b < a - qb - r \), which is a contradiction hence \( r < b \)

since there are \( r \) and \( b \) and \( r < b \), the contradiction proves existence
proof of uniqueness

show that, if there are two representations of a, \(a = qb + r = q'b + r'\), where \(0 \leq r, r' < b\), then \(r = r'\) and \(q = q'\)

take: \(qb + r = q'b + r'\) rearrange: \(r' - r = q(b - b')\)*

take absolute value: \(|r' - r| = q|b - b'||**

but \(0 \leq r' < b\), since \(r' < b\), and \(-b < r < 0\), since \(-b < r\)

so \(-b < r' - r < b\) \(|r' - r| < b|***

so, by ** and ***, \(b|q - q'| < b\), \(|q - q'| < 1\) hence \(q = q'\) and, by *, \(r = r'\)

the equality of variables proves uniqueness

General Division Theorem

let \(a\) and \(b\) be integers, where \(b \neq 0\)

let there be unique integers \(q\) and \(r\) such that \(a = qb + r\) and \(0 \leq r \leq |b|\)

proof:

two cases, since \(|b| > 0\), \(b > 0\) and \(b < 0\)

we have proven the result for \(b > 0\), so assume \(b < 0\)

since \(|b| > 0\), previous theorem suggests there are unique integers \(q'\) and \(r'\) such that \(a = q'|b| + r'\) and \(0 \leq r' < |b|\)

let \(q = -q', r = r'\) then, since \(|b| = -b\), we get \(a = qb + r\) and \(0 \leq r < |b|\)

officially, \(q\) is called the quotient of \(a\) by \(b\), and \(r\) is called the remainder

\(a\) = dividend, \(b\) = divisor, \(q\) = quotient, \(r\) = remainder

Divisibility

if division of \(a\) by \(b\) produces a remainder \(r = 0\), we say \(a\) is divisible by \(b\)

hence, \(a\) is divisible by \(b\) iff there is an integer \(q\) such that \(a = bq\) and \(r = 0\)

\(b|a\) iff \(\exists q[a - bq]\), where \(b \neq 0\) \((b\) divides \(a\) if and only if there is an integer \(q\) such that \(a = bq\) and \(b \neq 0\))

eg. \(45\) is divisible by \(9\) \((9|45)\), but \(44\) is not divisible by \(9\) \((9\nmid 44)\)

notation. \(b|a\) denotes \(a\) is divisible by \(b\) \((b\) divides \(a\))

warning. \(b|a\) is not the same as \(b/a\)

\(b|a\) - Boolean property - relationship between \(a\) and \(b\) \((\text{divisor divides dividend})\) true or false

\((\text{divisor}|\text{dividend})\) \(|\) - divides \((\text{is divisible by})\)

\(b/a\) - rational number - the result of dividing \(b\) by \(a\) in the rational number set \((\text{number} (\text{value}))\)

\((\text{dividend}/\text{divisor})\) / - divided by

Basic Properties of Divisibility

theorem. let \(a, b, c\) and \(d\) be integers, where \(a \neq 0\) then.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(a</td>
<td>0) and (a</td>
<td>a)</td>
</tr>
<tr>
<td>3</td>
<td>if (a</td>
<td>b) and (c</td>
<td>d), then (ac</td>
</tr>
<tr>
<td>5</td>
<td>(a</td>
<td>b) and (b</td>
<td>a) iff (a = \pm b)</td>
</tr>
<tr>
<td>7</td>
<td>if (a</td>
<td>b) and (a</td>
<td>c), then (a</td>
</tr>
</tbody>
</table>

proofs of the basic properties of divisibility

each of the properties is proved using \(a|b \iff \exists q[a - bq]\)

proof for 4. let there be \(\exists d\) and \(\exists c\) such that \(b = da\) and \(c = eb\) by substitution \(c = (ed)a\) hence \(a|c\)

proof for 6. since \(a|b\), there is \(\exists d\) such that \(b = da\) so \(|b| = |d|\) \(|a|\) since \(b \neq 0\), \(|d| \geq 1\) so \(|a| \leq |b|\)
Prime Number
a prime number is an integer \( p > 1 \) that is divisible only by 1 and \( p \)

Fundamental Theorem of Arithmetic (revisited)

Theorem. Every natural number greater than one is either prime or can be expressed as a product of primes in a way that is unique except for the order in which they are written.

Example: \( 4 = 2 \times 2 \), \( 6 = 2 \times 3 \), \( 8 = 2^3 \), \( 9 = 3^2 \), \( 10 = 2 \times 5 \), \( 12 = 2^2 \times 3 \), ..., \( 3366 = 2 \times 3^2 \times 11 \times 17 \), ...

Prime decomposition - the expression of a number as a product of primes

Proof. Existence and uniqueness.

Existence: All natural numbers > 1 are either prime or products of primes.

Proof by induction: done earlier.

Proof by contradiction:

Suppose there were a composite number (not prime) that cannot be written as a product of primes.

Then there must be a smallest such number, call it \( n \). Since \( n \) is composite, it is not prime.

Since \( n \) is not prime, there are numbers \( a \) and \( b \) with \( 1 < a, b < n \) such that \( n = ab \).

Case 1: If \( a \) and \( b \) are primes, then \( n = ab \) is a prime decomposition of \( n \) and we have a contradiction.

Case 2: If either of \( a \) or \( b \) (or both) is composite and less than \( n \), it must be a product of primes.

Replace one or both of \( a \) and \( b \) by its prime decomposition in \( n = ab \).

Get a prime decomposition of \( n \), and again we have a contradiction.

This proves existence, by contradiction and downward proof.

Uniqueness: The prime decomposition of any natural number \( n > 1 \) is unique up to the ordering of the primes.

Proof by contradiction:

Assume there is a number > 1 that has two (or more) distinct prime decompositions.

Let \( n \) be the smallest such number.

Let \( n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \) be two different prime decompositions of \( n \).

Since \( (p_1)(p_2 \cdots p_r) = q_1 q_2 \cdots q_s \), \( p_i \) divides \( q_1 q_2 \cdots q_s \).

By Euclid's Lemma.

Euclid's Lemma. If a prime \( p \) divides a product \( ab \), then \( p \) divides at least one of \( a \) or \( b \).

Either \( p_i | q_1 \) or \( p_i | (q_2 \cdots q_s) \) or both.

So, a common factor must exist.

Hence, either \( p_i | q_1 \) or else \( p_i | q_i \) for some \( i \) between 2 and \( s \).

But then we can delete \( p_i \) and \( q_i \) from the two decompositions in *.

This gives us a number smaller than \( n \) that has two different prime decompositions.

Contradiction to the choice of \( n \) as the smallest such.

This proves uniqueness, by contradiction, using Euclid's Lemma.

Hilbert's Hotel

Infinite rooms numbered naturally.

One night all rooms occupied, one new customer can fit without ejecting anyone.

Move everyone into next room \( n \rightarrow n+1 \).

Variants: Two guests arrive, separate rooms.

Infinite tour group, each member = \( n \).

Infinite - key to calculus.
Lesson 11 – Elements of Real Analysis

History

counting (discrete) and measurement (continuous) activities predate numbers (abstractions for communication)
pre-19th C: what is the quotient of a/b? no such concept
19th C: real number system connected numbers integers → rationals → real

Properties of Rationals

theorem: if r and s are rationals, with r < s, then there is a rational t such that r < t < s
this property is called density the rational line is dense
proof that the rational line is dense:

let t = (r+s)/2 clearly r < t < s
is t ∈ Q?
let rationals r = m/n and s = p/q, where m, n, p and q are integers
then t = (m/n + p/q)/2 = (mq + np)/(2nq)
by multiplication of integers, mq, np and 2nq are integers
so t ∈ Q QED

in a similar proof, one can show the integer line is dense as well

The Case for Irrationals

density does not mean there are no holes in the rational line same for integer line (integers → rationals)
example. \( \sqrt{2} \)

let A = \{ x ∈ Q | x ≤ 0 ∨ x^2 < 2 \} let B = \{ x ∈ Q | x > 0 ∧ x^2 ≥ 2 \}
clearly A ∪ B = Q, but A has no greatest member and B has no smallest member
hence, the rationals are inadequate to do mathematics
in Q, we cannot solve the equation \( x^2 - 2 = 0 \)

mind-blowing way out. find way to fill in the holes in Q \( \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \)
discover: holes in rational number line outweigh rational numbers on line same for holes in integer line
so irrationals (\( \mathbb{I} \)) introduced
two levels of infinity internal infinity (infinite density) and external infinity (unending domain)

Intervals of the Real Line

let a ∈ R, b ∈ R and a < b
the open interval (a,b) is the set \{ x ∈ R | a < x < b \} a and b ∉ (a,b) big distinction
the closed interval [a,b] is the set \{ x ∈ R | a ≤ x ≤ b \} a and b ∈ [a,b]
variations of notation
half-open or half-closed \[ a,b \] - \{ x ∈ R | a ≤ x < b \} left-closed, right-open
\( a,b \] - \{ x ∈ R | a < x ≤ b \} left-open, right-closed
\( -\infty,a \] - \{ x ∈ R | x < a \} \( -\infty,a \] - \{ x ∈ R | x ≤ a \} \( a,\infty \] - \{ x ∈ R | x > a \} \( a,\infty \] - \{ x ∈ R | x ≥ a \}
cannot have \[ -\infty,a \], \( -\infty,a \], (a,\infty] nor [a,\infty] because is not a real number, so it cannot be part ( nephew ) of any set
Key Property of Real Numbers

- trivial often means profound (this property opens up mathematics)

Completeness Property - no gaps within

the completeness property of the real number system (\( \mathbb{R} \)) says that every nonempty set of reals that has an upper bound has a least upper bound in \( \mathbb{R} \)

given a set \( A \) of real numbers, a number \( b \) such that \( (\forall a \in A) \ [a \leq b] \) is said to be an upper bound of \( A \)

we say \( b \) is a \textit{least upper bound} of \( A \) if, in addition, for \textit{any} upper bound \( c \) of \( A \), we have \( b \leq c \)

notation: least upper bound (of \( A \)) - \( \text{lub}(A) \)

real intervals have an infinite number of upper bounds

in a right-open real interval, we can get infinitesimally close(r) to the right-excluded number, and so have infinite apparent upper bounds

the least of these is \( \text{lub} \) \( \text{lub} \) is not a member of a right-open interval \( \text{lub} \neq \text{max} \) in set (\( \text{lub} > \text{max} \))

the right-closed real interval seems intuitively to have only one upper bound, the right-most included number however, there are infinite upper bounds, since numbers outside of the interval are also upper bounds, and, since there are an infinite many of them, there are an infinite number of upper bounds

the least of these is \( \text{lub} \) \( \text{lub} \) is the right-most included number (\( \text{max} \))

the same arguments can be made for lower bounds, greatest lower bound (\( \text{glb} \)), natural numbers, integers and rationals

Theorem: the rational line is not complete  completeness. if \( A \subset \mathbb{R} \) has an upper bound, then it has a lub in \( \mathbb{R} \)

proof. show that \( A \) has no lub

let \( A = \{ r \in \mathbb{Q} \mid r \geq 0 \land r^2 < 2 \} \) \( A \) is bounded above \( 2 \) is an upper bound

show \( A \) has an upper bound

rewrite \( A \) \( \{0, \sqrt{2}\} \) in \( \mathbb{Q} \) so \( A = \{ r \in \mathbb{Q} \mid 0 \leq r < \sqrt{2} \} \)

no rational number \( r \) in \( A \) is higher than \( \sqrt{2} \)

\( \sqrt{2} \) is an upper bound of \( A \)

since \( \sqrt{2} \approx 1.41 \), 1.4 or 7/5 is a rational upper bound of \( A \)

\( A \) has an upper bound

show \( A \) does not have a least upper bound (lub)

Case 1. \( \text{lub} \neq \sqrt{2} \) since \( \sqrt{2} \notin \mathbb{Q} \)

Case 2. assume \( \text{lub} > \sqrt{2} \) (external to \( A \))

let \( x \in \mathbb{Q} \) be \textit{any} rational upper bound of \( A \) lower than \( 2 \) and higher than \( \sqrt{2} \)

such as \( \frac{2n}{(n+1)} \) for \( n \in \mathbb{N} \) so \( 2 \) is not the lub for \( A \)

let \( y \in \mathbb{Q} \) be \textit{any} rational upper bound of \( A \) lower than \( x \) and higher than \( \sqrt{2} \)

such as \( \frac{xm}{(m+1)} \) for \( m \in \mathbb{N} \) so \( x \) is not the lub for \( A \)

can repeat ad infinitum

\( \text{lub} \neq \sqrt{2} \) so \( \text{lub} \leq \sqrt{2} \) but, by Case 1, \( \text{lub} \neq \sqrt{2} \) so \( \text{lub} < \sqrt{2} \)

Case 3. assume \( \text{lub} < \sqrt{2} \) (internal to \( A \))

let \( a \in A \) be \textit{any} rational number between lub and \( \sqrt{2} \)

such as \( \frac{[hn/(h+1)]}{(h+1)/h} \) for \( h \in \mathbb{N} \) so \( a > \text{lub} \)

but then lub is no longer an upper bound of \( A \), since \( a > \text{lub} \) and an upper bound of \( A \)

let \( b \in A \) be \textit{any} rational number between \( a \) and \( \sqrt{2} \) same result can repeat ad infinitum

\( \text{lub} < \sqrt{2} \) so \( \text{lub} \geq \sqrt{2} \) but, by Case 1, \( \text{lub} \neq \sqrt{2} \) and, by Case 2, \( \text{lub} \neq \sqrt{2} \)

so \( A \) has no least upper bound (lub)
the construction of \( \mathbb{R} \) from \( \mathbb{Q} \) can be done in several different ways, but in all cases the aim is to prevent an argument like the above going through for \( \mathbb{R} \).

### Real Number Sequences

A sequence is a list, such as \( a_1, a_2, a_3, \ldots \), (infinite sequence tends to infinite, no limit)

\[
\begin{align*}
\mathbb{N} & = 1, 2, 3, \ldots \to \{ n \in \mathbb{N} \} \\
7, 7, 7, \ldots & = \{ 7 \} \in \mathbb{N}
\end{align*}
\]

3, 1, 4, 1, 5, 9, \ldots = the decimal digits of \( \pi \)

\[\left\{ (-1)^{n+1} \right\}_{(n=1)} \to -1, 1, -1, 1, \ldots \quad \text{(alternating sequence)}\]

### Limits of a Sequence

If the numbers in a sequence \( \left\{ a_n \right\}_{(n=1)} \) get arbitrarily close to some fixed number \( a \), we say \( \left\{ a_n \right\}_{(n=1)} \) tends to the limit \( a \) and write \( a_n \to a \) as \( n \to \infty \) or \( \lim_{n \to \infty} a_n = a \)

- \( \{1/n\}_{(n=1)} \to 1, 1/2, 1/3, 1/4, \ldots \) limits to 0 (tends arbitrarily close to 0) \( \lim_{n \to \infty} 1/n = 0 \)
- \( \{1+1/(2^n)\}_{(n=1)} \to 3/2, 5/4, 9/8, 17/16, \ldots \) limits to 1 (tends arbitrarily close to 1) \( \lim_{n \to \infty} 1+1/(2^n) - 1 \)
- \( 3, 3.1, 3.14, 3.1415, 3.14159, \ldots \) limits to \( \pi \) (tends arbitrarily close to \( \pi \))

### Formal Definition of the Limit of a Real Sequence

\[
\left\{ a_n \right\}_{(n=1)} \to a \quad \text{as} \quad n \to \infty \quad \text{so} \quad |a_n - a| \quad \text{becomes arbitrarily close to} \quad 0
\]

We say \( a_n \to a \) as \( n \to \infty \) iff \((\forall \varepsilon > 0)(\exists n \in \mathbb{N})(\forall m \geq n) \left\{ |a_m - a| < \varepsilon \right\} \) where \( \varepsilon \) is infinitesimal (close to 0)

Quantification order matters

Consider \((\exists n)(\forall m \geq n) \left\{ |a_m - a| < \varepsilon \right\}\)

This says from some point \( n \) onward, all the numbers in \( \left\{ a_n \right\}_{(n=1)} \) are within a distance of \( \varepsilon \) from a tolerance. The choice of \( n \) depends on \( \varepsilon \) so need to pick an \( n \) that allows \( \varepsilon \) to be infinitesimal

Intuition is that we can take \( \varepsilon > 0 \) as small as we want

Sequence tends to a

**all elements in the sequence that lie between** \( a - \varepsilon \) **and** \( a + \varepsilon \)

\[\begin{align*}
\text{all elements between} & \quad a - \varepsilon' \quad \text{and} \quad a + \varepsilon' \\
\text{all elements between} & \quad a - \varepsilon'' \quad \text{and} \quad a + \varepsilon'' \\
\text{all elements between} & \quad a - \varepsilon''' \quad \text{and} \quad a + \varepsilon''' \\
& \quad \vdots \\
\text{all elements between} & \quad a - \varepsilon'''' \quad \text{and} \quad a + \varepsilon'''' \\
& \quad a - \varepsilon'''' \to a + \varepsilon'''' \quad \forall \varepsilon
\end{align*}\]

Prove \( \{1/n\}_{(n=1)} \), \( 1/n \to 0 \) as \( n \to \infty \) rigorously

\((\forall \varepsilon > 0)(\exists n \in \mathbb{N})(\forall m \geq n) \left\{ |1/m - 0| < \varepsilon \right\} \)

Let \( \varepsilon > 0 \) be arbitrarily given we need to find an \( n \) such that \((\forall m \geq n) \left\{ |1/m| < \varepsilon \right\}\)

Pick any \( n \) such that \( n > 1/\varepsilon \) by the Archimedean Property, if \( m \geq n, \ 1/m \leq 1/n < \varepsilon \)

Archimedean Property: \((\exists x \in \mathbb{R}) (\exists y \in \mathbb{R}) (x > 0) \land (y > 0) \Rightarrow (\exists n \in \mathbb{N}) \left[ nx > y \right]\)

Prove \( \{n/(n+1)\}_{(n=1)} \to 1/2, 2/3, 3/4, 4/5, \ldots \) tends to 1

\((\forall \varepsilon > 0)(\exists n \in \mathbb{N})(\forall m \geq n) \left\{ |m/(m+1)| - 1| < \varepsilon \right\} \)

Let \( \varepsilon > 0 \) be given we need to find an \( n \) such that for all \( m \geq n, \ |m/(m+1)| - 1| < \varepsilon \)

Pick \( n \) so large that \( n > 1/\varepsilon \) then for any \( m \geq n, \ |m/(m+1)| - 1| - |(-1)/(m+1)| - 1/(m+1)| < 1/m \leq 1/n < \varepsilon \)

With this, mathematics opens up and we are able to explore deeper mathematical patterns (e.g. now can do calculus) QED