Course webpage

- Profile of class
  - algebra > number theory > analysis
  - most of the main ideas are new to at least two-thirds of the class, especially the set theory
  - introductory notes on implication
  - gentle lead-in to the Propositional Calculus

- Exercises for Week 2 (stand problems (as outline)

- Assessment into
  - 1st assignment due Week 6 15%
  - peer assessment Week 8 5%
  - 2nd assignment due Week 10 10%
  - peer assessment Week 12 5%

- exam 60%

No quit next week or any week!!
Example of Peer Review: Student wrote

**Claim:** Blah blah blah is true

**Proof:**

\[ (1-a)m + cm = 1 \]

\[ \Rightarrow \quad \text{Super-duper blah blah is true} \]

\[ \Rightarrow \quad \text{Blah blah blah is true.} \]

- Apart from this error, proof is correct and sophisticated.

- Something else that is blatantly false.

- How to grade this?
Variation on diagonalization:

Recall Russell's Paradox

Put $S = \{ x \mid x \notin x \}$

Then $S$ is not a set.

Proof: If $S$ is a set then $S \in S$ or $S \notin S$ and both possibilities yield contradictions.

Hence $S$ is not a set.

However $S$ is a class, thought not one to which set membership "$\in$" can be applied.

The idea of Russell's paradox has many variations which can be loosely grouped into the title "diagonalization arguments".

\[ y \mapsto y \notin y \]

"Diagonalize the diagonal!!"
Early example (Euclid): There are infinitely many primes.

Proof: Suppose there are finitely many primes, $p_1, \ldots, p_n$. Put

$$q = (p_1 \cdots p_n) + 1$$

Then $p_1 \nmid q$, $p_2 \nmid q$, $\ldots$, $p_n \nmid q$ (since remainder is 1 when divided). Thus $q$ is not composite, so $q$ is prime.

Hence $q = p_i \implies q > p_n$.


[Boxed text: Shocking 19th century example (Cantor): There are uncountably (infinitely) many real numbers.]
A set \( X \) is called **countable** if \( X \) is finite or in a one-to-one correspondence with \( \mathbb{Z}^+ \) via a bijection.

where
\[
\mathbb{Z}^+ = \{1, 2, 3, \ldots\}
\]

A set is called **uncountable** if it is not countable (in particular, if infinite).

**Proof that \( \mathbb{R} \) is uncountable**

Suppose \( \mathbb{R} \) is countable so can be listed

\[
x_1 = \ldots d_{11} d_{12} d_{13} d_{14} \ldots
\]
\[
x_2 = \ldots d_{21} d_{22} d_{23} d_{24} \ldots
\]
\[
x_3 = \ldots d_{31} d_{32} d_{33} d_{34} \ldots
\]
\[
x_4 = \ldots d_{41} d_{42} d_{43} d_{44} \ldots
\]

Put
\[
y = 0 \cdot e_1 e_2 e_3 e_4 \ldots
\]

where \( e_i \neq d_{ii} \) for \( i = 1, 2, \ldots \) and \( e_i \notin \{0, 1, 2, \ldots\} \).
Then $y \in \mathbb{R}$ so $y = \alpha_j \cdot \frac{1}{e^n} \quad \exists \alpha \in \mathbb{Z}^+$, so

$$0 \cdot e_1 e_2 \ldots e_{j-1} e_j e_{j+1} \ldots = \ldots \cdot d_1 d_2 \ldots d_{j-1} d_j \ldots$$

all different digits.

Hence $e_j = 0$ or $9$. 

Hence $\mathbb{R}$ is uncountable.

Note: $0.999 \ldots = 1.000 \ldots$

Decimal expansions of reals are unique except for repeating 9s and 0s.

Corollary: $|\mathbb{R}| > |\mathbb{Z}^+| = |\mathbb{N}|$

infinite cardinalities
Continuum Hypothesis: There is no cardinality between $\mathbb{Z}^+$ and $|\mathbb{R}|$.

Remarkably unresolved!!!

Google: continuum hypothesis Woodin

What about $\Theta$? $\Theta = \gamma$ relevant?

Consider $\mathbb{Q}^+$:

\[ \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{3}{4}, \frac{3}{5}, \frac{4}{5}, \frac{5}{6}, \ldots \]

Every possible rational $\frac{m}{n}$ lies on this list.

Since $\frac{m}{n} \in \{ \frac{1}{m+n+1}, \frac{2}{m+n+2}, \ldots, \frac{k}{m+n+k} \}$, etc.

\[ \frac{m}{n} \implies \frac{m}{m+n} = \frac{m}{n+1}, \ldots, \frac{m}{m+n-1}, \ldots, \frac{m}{m+n+k} \]
Ignore duplicates and we have a listing of $\mathbb{Q}^+$.

It is a bijection

$$f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$$

$$n \mapsto f(n) = \text{with rational } n \in \mathbb{Z}^+.$$

Define $g : \mathbb{Z}^+ \rightarrow \mathbb{Q}$ by

$$g(n) = \begin{cases} 0 & \text{if } n = 1 \\ f(\frac{n}{2}) & \text{if } n \text{ even} \\ -f\left(\frac{n-1}{2}\right) & \text{if } n \text{ odd, } n \geq 3 \end{cases}$$

Check: $g$ is a bijection

This leads to a well-ordering of $\mathbb{Q}$

See later in course.

In particular $|\mathbb{Q}| = |\mathbb{Z}^+|$.

(No contradiction to Continuum Hypothesis).