Contradiction

- How to be so wrong that you end up being right

> **Problem 1**
> Let $a, b, c, d \in \mathbb{Z}$. Show that if $a^2 + b^2 = c^2$, then a or b is even.

- Take negation, $a^2 + b^2 = c^2$ and a and b are odd
- Let $a = 2j + 1$ and $b = 2k + 1$, $j, k \in \mathbb{Z}$
- $a^2 + b^2 = (2j+1)^2 + (2k+1)^2 = 4(j^2 + k^2) + 4(j + k) + 2 = 4(k^2 + j^2 + k + j) + 2$
- So we have $2 \equiv c^2 \pmod 4$
- We must show that this is impossible

> **Proof 1**
> Proof by contradiction: Assume a and b are odd
> Let $a = 2j + 1$ and $b = 2k + 1$, $j, k \in \mathbb{Z}$
> Then $a^2 + b^2 = c^2 \Rightarrow 4(k^2 + j^2 + k + j) + 2 = c^2$
> We get $2 \equiv c^2 \pmod 4$
> Now $0^2 \equiv 0 \pmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 0 \pmod 4$ and $3^2 \equiv 1 \pmod 4$
> So there is no $c \in \mathbb{Z}$ s.t. $c^2 \equiv 2 \pmod 4$ $\Rightarrow\!\Leftarrow$

- Another way instead of modular arithmetic
- We notice that $2 \mid c^2 \Rightarrow 2 \mid c$ so we write $c = 2l, l \in \mathbb{Z}$
- So we get $4k^2 + 4j^2 + 4k + 4j + 2 = 4l^2$
- $\Rightarrow 4(k^2 + j^2 + k + j - l^2) = -2$
- $\Rightarrow 4 \mid -2$ this is a contradiction because 4 does not divide -2 $\Rightarrow\!\Leftarrow$

> **Procedure**
>
> - Assume the negation you want to prove
> - Do some math
> - Obtain a contradiction
> - Conclude the assumption is false

> **Example**

Prove that $\sqrt{2}$ is irrational

Prove by contradiction: Assume $\sqrt{2} \in \mathbb{Q}$. Then $\exists a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1$ s.t. $\sqrt{2} = \frac{a}{b}$

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

So $2 \mid a^2$. Recall if p is prime and $m, n \in \mathbb{Z}$ then $p \mid mn \Rightarrow p \mid m \vee p \mid n$

So we write $a = 2k, k \in \mathbb{Z}$, then $2b^2 = 4k^2 \implies b^2 = 2k^2 \implies 2 \mid b^2 \implies 2 \mid b$

This is a contradiction since $\gcd(a, b) = 1$. So $\sqrt{2} \notin \mathbb{Q}$

- Now lets try this with $\sqrt{7}$
  - Assume $\sqrt{7} \in \mathbb{Q}$. Then $\exists a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1$ s.t. $\sqrt{7} = \frac{a}{b}$
  - Then we have $7b^2 = a^2$
  - $7 \mid a^2$ so $7 \mid a, a = 7k, k \in \mathbb{Z}$
  - So we have $7b^2 = 49k^2$
  - Then $b^2 = 7k^2 \implies 7 \mid b$
  - This is a contradiction since $\gcd(a, b) = 1$. So $\sqrt{7} \notin \mathbb{Q}$
- And again for $\sqrt{49}$
  - Assume $\sqrt{49} \in \mathbb{Q}$. Then $\exists a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1$ s.t. $\sqrt{49} = \frac{a}{b}$
  - Then we have $49b^2 = a^2$
  - $49 \mid a^2$ so $49 \mid a, a = 49k, k \in \mathbb{Z}$, proof fails here because 49 is not prime so the statement $49 \mid a^2 \implies 49 \mid a$ may not be true
  - But we have $7 \mid a, a = 7k, k \in \mathbb{Z}$
  - Then $49b^2 = 49k^2 \implies b^2 = k^2$ so this also doesn't work

Problem 2

Let $\mathbb{I}$ be the set of irrational numbers. That is $\mathbb{I} = \mathbb{R} - \mathbb{Q}$

Prove the following statements

1. Let $x \in \mathbb{R}$. If $x \in \mathbb{I}$ then $\frac{1}{x} \in \mathbb{I}$
2. Let $n \in \mathbb{Z}$ and $x \in \mathbb{R}$. If $x \in \mathbb{I}$ then $n + x \in \mathbb{I}$

Solution

1. Proof by contradiction: Assume $\frac{1}{x} \in \mathbb{Q}$. Then $\frac{1}{x} = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$. Note that $a \neq 0$, otherwise $\frac{1}{x} = 0 \implies 1 = 0$ which is silly
   Then $\frac{1}{x} = \frac{a}{b}$ rest of proof is in lecture 21 notes
2. Proof by contradiction: Assume $n + x \in \mathbb{Q}$.
   So $n + x = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$
   $\implies x = \frac{a-nb}{b}$
   Since $(a - nb), b \in \mathbb{Z}, x \in \mathbb{Q}$. This is a contradiction

- Make sure you do the question on the slides because it is a hard finals question