PLP - 38

TOPIC 38—TWO VERY FAMOUS PROOFS

Demirbaş & Rechnitzer

IRRATIONALITY OF $\sqrt{2}$

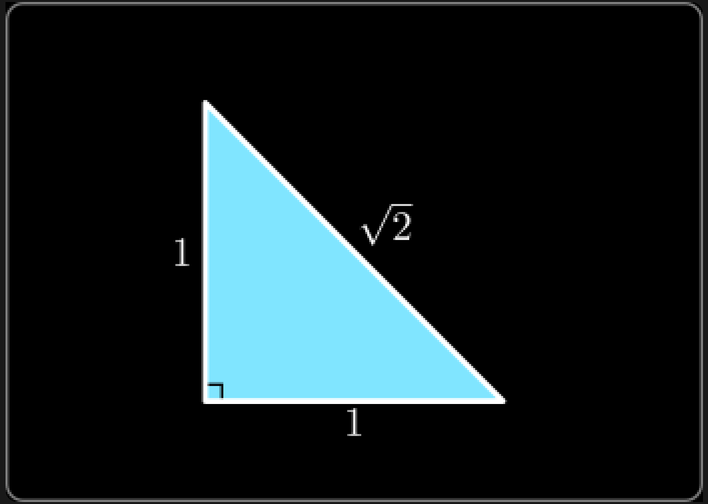
IRRATIONALITY OF $\sqrt{2}$

THEOREM: (HIPPASUS 500BC?).

The real number $\sqrt{2}$ is not rational

This is one of the most famous results in mathematics

- Existence of $\sqrt{2}$ as a real quantity follows from Pythagoras' Theorem
- This was first proof that there are reals that are not rational
- It was, and is, a big deal!



We'll need

Let $n \in \mathbb{N}$. Then n is even if and only if n^2 is even.

SCRATCHWORK

$\sqrt{2}$ is irrational

Scratchwork

- Do proof by contradiction, so we can write $\sqrt{2} = a/b$ with $a, b \in \mathbb{Z}$
- Rearrange this to get $a = \sqrt{2}b$
- Square it to get rid of the $\sqrt{\cdot}$ $\qquad a^2 = 2b^2$
- But this means a is even. So we can write $a = 2c$
- This tells us $2b^2 = 4c^2$ and so $b^2 = 2c^2$.
- This means that b is even
- Hold on — can't we just make sure a, b have no common factors?

PROOF

$\sqrt{2}$ is irrational

PROOF.

Assume, to the contrary, that $\sqrt{2} \in \mathbb{Q}$. Hence we can write $\sqrt{2} = \frac{a}{b}$, so that $b \neq 0$ and $\gcd(a, b) = 1$

Since $\sqrt{2} = \frac{a}{b}$ and so $a^2 = 2b^2$. Thus a^2 is even, and so a is even. Hence write $a = 2c$ where $c \in \mathbb{Z}$

But now, since $a^2 = 2b^2$, we know that $4c^2 = 2b^2$ and so $b^2 = 2c^2$. Hence b^2 is even, and so b is even.

This gives a contradiction since we assumed that $\gcd(a, b) = 1$. Thus $\sqrt{2}$ is irrational.

PRIMES ARE INFINITE

PRIMES FOREVER

PROPOSITION: (EUCLID 300BC).

There are an infinite number of primes.

We prove this by contradiction, but need the following result along the way

LEMMA:

Let $n \in \mathbb{N}$. If $n \geq 2$ then n is divisible by a prime.

AT LEAST ONE PRIME DIVISIOR

Let $n \in \mathbb{N}$. If $n \geq 2$ then n is divisible by a prime.

PROOF.

We prove this by strong induction.

- Base case: Since 2 is prime and $2 \mid 2$, the result holds when $n = 2$.
- Inductive step: Let $k \in \mathbb{N}$ with $k \geq 2$, and assume that the result holds for all integers $2, 3, \ldots, k$.
    - If $k+1$ is prime then since $(k+1) \mid (k+1)$, the result holds at $n = k+1$
    - If $k+1$ is not prime, then $(k+1) = ab$ for integers $a, b \geq 2$. But, by assumption, both a, b have prime divisors, and so $a = pc, b = qd$ where $c, d \in \mathbb{N}$ and p, q prime. Hence $(k+1) = pqcd$ and so the result holds at $n = k+1$

Since the base case and inductive step hold, the result follows by induction.

PROOF OF INFINITE PRIMES

There are an infinite number of primes.

PROOF.

Assume, to the contrary, that there is finite list of primes: $\{p_1, p_2, \ldots, p_n\}$.

Use this list to construct $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n \in \mathbb{N}$, and then consider $(N+1)$.

- If $(N+1)$ is prime, then we have found a new prime larger than all on our list — contradiction!
- If it is not prime, then (by lemma) $(N+1)$ has some p_k as a divisor.

  But then $p_k \mid N$ and $p_k \mid (N+1)$, and so

$$1 = (N+1) - N = (p_k b) - (p_k a) = p_k(b-a) \qquad \text{for some } a, b \in \mathbb{N}$$

  which implies that $p_k \mid 1$ — contradiction!

So the list cannot be finite.