Announcements

1) Reading Quiz for today does not expire!

2) HW3 due next Tuesday

Proof by Contradiction

Section 3.3

Definition: (contradiction) A **contradiction** is a compound statement that is always false, independent of the truth value of its components

Easiest contradiction: $P \wedge (\neg P)$

How it works (reductio ad absurdum)

Given a conclusion, you assume the negation. You reason from the negation to a contradictory statement (often $P \wedge (\neg P)$)

Since this kind of statement is always false, your assumption of the negation must be false.

Example 1: Prove that there are infinitely many prime numbers

proof: By contradiction! Suppose there are finitely many prime numbers $p_1, p_2, \ldots, p_n$.

Let $\boxed{x = (p_1 p_2 \cdots p_{n-1} p_n) + 1}$.

None of p_i, $1 \leq i \leq n$, divide x since the remainder is one.

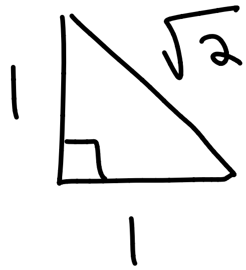
Therefore, either x itself is prime or there is another prime p_{n+1} where $p_{n+1} \mid x$.

In either case, we have both n and $n+1$ prime numbers, contradiction. Therefore, there are infinitely many prime numbers.

$\square$

Example 2: $\sqrt{2}$ is irrational

Note:



proof: By contradiction. Suppose $\sqrt{2}$ is rational. Therefore, $\exists\ m, n \in \mathbb{Z},\ n \neq 0$, with

$$\sqrt{2} = \frac{m}{n}.$$

Square both sides.

$$2 = \frac{m^2}{n^2}, \quad \text{so}$$

$$2n^2 = m^2.$$

There are an <u>even</u> number of 2's in the factorization of m^2.

(If $m = 2^k b$, $2 \nmid b$, then

$$m^2 = (2^k)^2 b^2 = 2^{2k} b^2,$$

$2k$ two's in the factorization)

Similarly, there are an even number of 2's in the factorization of n^2.

(If $n = 2^{\ell} a$, $2 \nmid a$, then

$n^2 = 2^{2\ell} a^2$, 2ℓ twos)

Therefore, $2n^2 = 2^{2\ell+1} a^2$,

$2\ell+1$ twos, which is an odd number of twos.

Since m^2 has $2k$ twos, if $m^2 = 2n^2$, then $2\ell+1 = 2k$ and so we have a number that is both even and odd, contradiction.

Therefore, $\sqrt{2}$ is irrational.

$\square$