CS 222 Lec 5

Proofs

- proving something is both an art and a science.

art → idea for strategy to find proof

science → logically correct

Proofs about Numbers

Divisibility

Defn Let $n \neq 0$ be an integer

We say n is divisible by q if $\exists\, k \neq 0$ (integer) s.t.

$$n = k \cdot q$$

Shorthand: $q \mid n$
"q divides n"

<u>Proposition</u>

$(\equiv \forall n \in \mathbb{Z}, \forall m \in \mathbb{Z})$

$$\forall\, n, m \in \mathbb{Z}$$

$$\underbrace{k \mid n,\ k \mid m}_{p} \Rightarrow \underbrace{k \mid (m+n)}_{q}$$

"For all integers n and m, if k divides n and k divides m then k divides $(m+n)$."

<u>Proof</u>

Let m be some integer
Let n be some integer.

Assume $k \mid n$ and $k \mid m$.

By the defn of divisibility,

$\exists\, q_1$ such that $n = q_1 \cdot k$
$\exists\, q_2$ such that $m = q_2 \cdot k$

Let's write

$$(n+m) = q_1 \cdot k + q_2 \cdot k$$
$$= (q_1 + q_2) \cdot k$$

So $n+m$ is divisible by k.

So, $k \mid n,\ k \mid m \Rightarrow k \mid (n+m)$

$\square$

"end of proof"

Rational Numbers

Defn A number r is rational if $\exists\, a, b \in \mathbb{Z}$ $(b \neq 0)$ such that

$$r = a/b$$

Properties

Prop. Let r_1, r_2 be rational numbers. Then $r_1 + r_2$ is a rational number.

Proof Since r_1 is rational we can write $r_1 = a_1/b_1$ $(b_1 \neq 0)$

Likewise, $r_2 = a_2/b_2$ $(b_2 \neq 0)$

$$(r_1 + r_2) = \frac{a_1}{b_1} + \frac{a_2}{b_2}$$

$$= \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

$b_1 b_2 \neq 0$ since $b_1 \neq 0$ and $b_2 \neq 0$

$$r_1 + r_2 = c/d$$

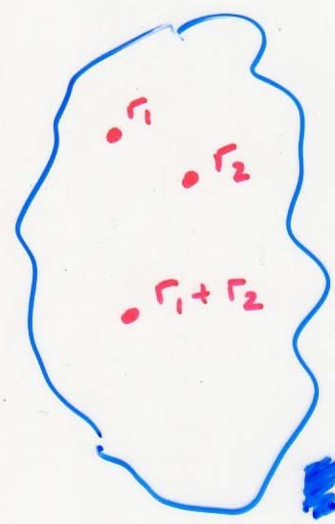
$$c = a_1 b_2 + a_2 b_1 \in \mathbb{Z}$$

$$d = b_1 b_2 \in \mathbb{Z}, \quad d \neq 0$$

So $r_1 + r_2$ is rational.

$\square$

Aside



$\mathbb{Q}$ = set of all rational numbers

We say $\mathbb{Q}$ is closed under $+$.
(and $-$, $*$, $/$?)
NO

Proof that $\forall n \in \mathbb{Z}$, $n^2 + n$ is even.

Proof #1

Case 1: n is even

$$n = 2K$$

$$\begin{aligned} n^2 + n &= (2K)^2 + 2K \\ &= 4K^2 + 2K \\ &= 2(\underbrace{2K^2 + K}_{\text{int.}}) \end{aligned}$$

So $n^2 + n$ is even.

Case 2: n is odd

$$n = 2 \cdot L + 1$$

$$\begin{aligned} n^2 + n &= (2L+1)^2 + (2L+1) \\ &= 4L^2 + 4L + 1 + 2L + 1 \\ &= 4L^2 + 6L + 2 \\ &= 2(\underbrace{2L^2 + 3L + 1}_{\text{int.}}) \end{aligned}$$

So $n^2 + n$ is even.

$\square$

Proof #2 $\quad n^2 + n = n(n+1)$

Either n is even or $n+1$ is even, so n^2+n is even.

$\square$

Division Theorem

$$\forall a, b \in \mathbb{Z} \quad \exists q, r \in \mathbb{Z}$$
$$0 \leq r < b$$

$$a = q \cdot b + r$$

$a = 20 \quad b = 10$

$q = 2 \quad r = 0$

$$20 = 2 \cdot 10 + 0$$

$a = 9 \quad b = 2$

$$9 = \underset{q}{\underline{4}} \cdot 2 + \underset{r}{\underline{1}}$$

$a = -15 \quad b = 10$

$$-15 = \underbrace{\boxed{-2}}_{q} \cdot 10 + \underbrace{\boxed{5}}_{r}$$

$9 \ \underline{\text{mod}} \ 4 = 1$

$-15 \ \underline{\text{mod}} \ 10 = 5$