Announcements

- Second HW released last Friday, due this Friday

  http://www.cs.uiuc.edu/class/sp10/cs173

Recap: How to prove/disprove statements

	Prove	Disprove
Existential statements $\exists x, \quad P(x)$	Show $P(x)$ is true for some specific x	Show $P(x)$ is false with a general argument
Universal statements $\forall x, \quad P(x)$	Show $P(x)$ is true with a general argument	Show $P(x)$ is false for some specific x

- *Examples from last time*:
  - $\exists x \in \mathbf{Q}, \; x^2 = 2.25$
  - $\forall x \in \mathbf{Q}, \; 2x \in \mathbf{Q}$

- Today's example: Show that the square of any odd number is odd

  - $\forall k \in \mathbf{Z_{odd}}, \; k^2 \in \mathbf{Z_{odd}}$ — Unpack/repack definition

  - $\forall k \in \mathbf{Z}, \; k \text{ is odd } \rightarrow k^2 \text{ is odd}$ — Proving an implication

Definitions of even and odd integers

- **Definition**: $n \in \mathbf{Z}$ is even if $\exists m \in \mathbf{Z},\ n = 2m$
- **Definition**: $n \in \mathbf{Z}$ is odd if $\exists m \in \mathbf{Z},\ n = 2m + 1$
- *Important*:
  - In definitions: "A if B" $\equiv$ $A \leftrightarrow B$
  - Everywhere else: "A if B" $\equiv$ "if B then A" $\equiv$ $B \rightarrow A$
- Is zero even or odd?
- **Proof that zero is even**: We need to show $\exists m \in \mathbf{Z},\ 0 = 2m$
  - For $m = 0 \in \mathbf{Z},\ 0 = 2m$
- **Proof that zero is *not* odd:** Need to show $\neg(\exists m \in \mathbf{Z},\ 0 = 2m + 1)$
  - $\forall m \in \mathbf{Z},\ 0 \neq 2m + 1$

$\forall k \in \mathbf{Z},\ k$ is odd $\rightarrow\ k^2$ is odd

- **Proof**: Suppose $k \in \mathbf{Z}$ and k is odd

  Then, by definition, $\exists m \in \mathbf{Z}, k = 2m + 1$

  Now $k^2 = (2m + 1)^2$
  $= (2m)^2 + 2(2m) + 1^2$
  $= 2(2m^2 + 2m) + 1$
  $= 2p + 1$, where $p = 2m^2 + 2m \in \mathbf{Z}$

  Hence, by definition, k^2 is odd

- **Observation**: We can use this result to show many other results:
  - If k is odd then k^4 is odd, k^8 is odd, k^{16} is odd, ...

- **Question**: Is the converse true? $\forall k \in \mathbf{Z},\ k^2$ is odd $\rightarrow\ k$ is odd

Disproving an existential statement

- Disprove the following: $\exists k \in \mathbf{Z},\ k^2 + 2k + 1 < 0$

- We need to prove: $\neg(\exists k \in \mathbf{Z},\ k^2 + 2k + 1 < 0)$
  $\equiv\ \forall k \in \mathbf{Z},\ k^2 + 2k + 1 \geq 0$

- **Proof**: Let $k \in \mathbf{Z}$

  Now $k^2 + 2k + 1$
  $= (k + 1)^2$
  ≥ 0, since the square of any integer is non-negative

Disproving a universal statement

- **Definition**: $r \in \mathbf{Q}$ is the multiplicative inverse of $q \in \mathbf{Q}$ if $qr = 1$
- Disprove: Every rational number has a multiplicative inverse
  $\forall q \in \mathbf{Q}, \exists r \in \mathbf{Q}$, r is the multiplicative inverse of q
- We need to prove: $\neg(\forall q \in \mathbf{Q}, \exists r \in \mathbf{Q}$, r is the mult. inverse of $q)$
  $\equiv \exists q \in \mathbf{Q}, \forall r \in \mathbf{Q}$, r is not the mult. inverse of q
- Complete the proof: Show that $q = 0$ "works"

Statements with multiple variables

- The product of two even integers is even
  $\forall j \in \mathbf{Z},\ \forall k \in \mathbf{Z},\ (j \text{ is even}) \wedge (k \text{ is even}) \rightarrow jk \text{ is even}$

- **Proof**: Let j and k be even integers

  Then, by definition, $\exists m \in \mathbf{Z},\ j = 2m$
  and $\exists n \in \mathbf{Z},\ k = 2n$

  Now $jk = (2m)(2n)$
  $= 2(2mn)$
  $= 2t$, where $t = 2mn \in \mathbf{Z}$

  Hence, by definition, jk is even