Spring 2015
Proof review session

How do you know there are an infinite number of primes?
I'll answer in haiku!

Top prime's divisors?

Product (plus one)'s factors are...?

Q.E.D., bitches!

Wow, after the 48-hour sleep-dep mark, lectures get really interesting.
the notion of proof: establishing truth

**Proof:** A formal argument establishing the truth of some proposition.

A proof should be **easy to verify**. But might be (very) hard to generate.

**P vs. NP question** [informal]: Can computers find proofs efficiently? (see CSE 421, 431)

Proof systems: Start with a basic set of axioms, and use inference rules to devise new theorems.

Which axioms to use is a tricky subject... see CSE 431.

We will talk about a related issue later: Undecidability of the halting problem.
inference rules

\[(p \land q) \rightarrow r \quad \neg \quad p \rightarrow r\]

\begin{tabular}{|c|c|}
\hline
\textbf{Modus Ponens} & \[\frac{p, \ p \rightarrow q}{\therefore q}\] \\
\hline
\textbf{Direct Proof} & \[\frac{p \Rightarrow q}{\therefore p \rightarrow q}\] \\
\hline
\textbf{Elim } \land & \[\frac{p \land q}{\therefore p, \ q}\] \\
\hline
\textbf{Intro } \land & \[\frac{p, \ q}{\therefore p \land q}\] \\
\hline
\textbf{Intro } \lor & \[\frac{p \lor q, \ \neg p}{\therefore q}\] \\
\hline
\textbf{Intro } \lor & \[\frac{p}{\therefore p \lor q, \ q \lor p}\] \\
\hline
\textbf{Excluded Middle} & \[\frac{\therefore p \lor \neg p}{\therefore q}\] \\
\hline
\textbf{Elim } \forall & \[\frac{\forall x P(x)}{\therefore P(a) \text{ for any } a}\] \\
\hline
\textbf{Intro } \forall & \[\frac{\text{Let } a \text{ be an arbitrary} \ldots}{\therefore \forall x P(x)}\] \\
\hline
\textbf{Elim } \exists & \[\frac{\exists x P(x)}{\therefore P(c) \text{ for some special } c}\] \\
\hline
\textbf{Intro } \exists & \[\frac{P(c) \text{ for some } c}{\therefore \exists x P(x)}\] \\
\hline
\end{tabular}
Show that \( q \rightarrow r \) follows from \( p \rightarrow r \) and \( q \rightarrow p \).

**Direct proof that \( q \rightarrow r \):**

1. \( q \)
2. \( p \rightarrow r \)
3. \( q \rightarrow r \)
4. \( p \)
5. \( r \)

\[ \quad \]

\[ 6. \quad q \rightarrow r \quad \] (optimal for top-level implication)
proofs using the direct proof rule

Show that \( r \) follows from \( q \) and \((p \land q) \rightarrow r\) and \( p \).

1. \( q \) given
2. \((p \land q) \rightarrow r\) given
3. \( p \) assumption
4. \( p \land q \) from 1 and 3 via Intro \( \land \) rule
5. \( r \) modus ponens from 2 and 4
6. \( p \rightarrow r \) direct proof rule
7. \( p \) given
8. \( r \) modus ponens from 6 and 7
proofs using the direct proof rule

Show that \( r \) follows from \( q \) and \((p \land q) \rightarrow r\) and \( p \).

1. \( q \) given
2. \((p \land q) \rightarrow r\) given
3. \( p \) assumption
4. \( p \land q \) from 1 and 3 via Intro \( \land \) rule
5. \( r \) modus ponens from 2 and 4
6. \( p \rightarrow r \) direct proof rule
7. \( p \) given
8. \( r \) modus ponens from 6 and 7

\( \neg p = p \) \( \neg \)
Prove that $p \rightarrow q$ follows from $r$ and $\neg(p \rightarrow \neg r) \rightarrow q$. 

$\text{Prove that } p \rightarrow q \text{ follows from } r \text{ and } \neg(p \rightarrow \neg r) \rightarrow q.$
cannot use inference rules inside propositions

1. $p \rightarrow q$  
   given

2. $(p \lor r) \rightarrow q$  
   intro $\lor$ from 1.

(Incorrect!)
universal vs. existential instantiation

Prove that $\exists x \ P(x)$ follows from $\exists x \ Q(x)$ and $\forall x \ (Q(x) \to P(x))$.

1. $\forall x \ (Q(x) \to P(x))$

2. $Q(a) \to P(a)$
   for a arbitrary |

3. $\exists x \ Q(x)$

4. $Q(c)$ for some specific $c$

---

1. $\exists x \ Q(x)$
2. $Q(c)$ for some specific $c$
3. $\forall x \ (Q(x) \to P(x))$
4. $Q(c) \to P(c)$
5. $P(c)$
6. $\exists x \ P(x)$
Prove that $\forall x (P(x) \rightarrow Q(x))$ and $\forall x (Q(x) \rightarrow R(x))$ implies $\forall x (P(x) \rightarrow R(x))$.

1. $\forall x (P(x) \rightarrow Q(x))$  
2. $\forall x (Q(x) \rightarrow R(x))$  
3. $P(a) \rightarrow Q(a)$  
   \hspace{1cm} \text{for some arbitrary } a  
4. $(Q(a) \rightarrow R(a))$  
5. $P(a)$  
6. $Q(a)$  
7. $R(a)$  
8. $P(x) \rightarrow R(x)$  
9. $\forall x (P(x) \rightarrow R(x))$
Prove that given $\forall x (P(x) \lor Q(x))$ and $\forall x \left( (\neg P(x) \land Q(x)) \rightarrow R(x) \right)$, then $\forall x (\neg R(x) \rightarrow P(x))$ is also true.
proof by contradiction: one way to prove \( \neg p \)

If we assume \( p \) and derive False (a contradiction), then we have proved \( \neg p \).

0. \( \neg p \)

1. \( p \) assumption

2. \( p \rightarrow F \) direct Proof rule

3. \( F \)

4. \( p \rightarrow F \) direct Proof rule

5. \( \neg p \lor F \) equivalence from 4

6. \( \neg p \) equivalence from 5
proof by contradiction

Prove that no whole number is both even and odd.

Pf. Assume f.t.s.o.c. \( \exists \) \( x \) s.t.

\( \text{Even}(x) \) and \( \text{odd}(x) \).

\( \Rightarrow \exists k, j \) integers s.t.

\[ x = 2k \]
\[ x = 2j + 1 \]

\( \Rightarrow \) \( 2k = 2j + 1 \)

\( \Rightarrow \) \( k = j + \frac{1}{2} \)

which is a contradiction b/c \( j + \frac{1}{2} \) is not an int if \( j \) is an int.
Prove that for all sets \( A, B, C \) such that \( C \neq \emptyset \), we have
\[ A \times C = B \times C \] if and only if \( A = B \).
Let $a, b$ be integers and $c, m$ be positive integers. Prove that if $ac \equiv bc \pmod{cm}$ then $a \equiv b \pmod{m}$. 