Announcements

• Homework 2 is due now.

• Homework 1 solutions are posted on the web site.

• Homework 3 will be posted by end-of-day tomorrow.
  • It is due Monday Feb. 23, in class.

• No class or office hours on Monday.
MATHEMATICAL PROOFS
Types of Proofs (we have seen so far)

Ways to prove “if $p$ then $q$”

• Direct proof
  • Assume $p$ is true
  • Use rules of inference, axioms, and logical equivalences to show that $q$ must also be true.

• Indirect proof – aka proof by contraposition
  • Assume $q$ is false.
  Use rules of inference, axioms, and logical equivalences to show that $p$ must also be false.
Types of Proofs (we have seen so far)

Ways to prove a proposition $r$ is true.

• Proof by contradiction.
  • First, assume that $r$ is false ($\neg r$ is true).
  • Then, show that $\neg r$ implies a contradiction, i.e.,
    $\neg r \rightarrow (s \land \neg s)$ for some proposition $s$. 
• **Theorem:** The difference between any rational number and any irrational number is irrational.

• **Proof:**
  • This is a proof by contradiction.
  • Assume that m is rational and n is irrational, but m-n is rational.
  • Since m is rational, \( m = \frac{a}{b} \) where \( a \) and \( b \) are integers with \( b \neq 0 \).
  • Similarly, since \( (m-n) \) is rational, \( (m-n) = \frac{c}{d} \), where \( c \) and \( d \) are integers with \( d \neq 0 \).
  • So, \( n = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \), where \( ad-bc \) and \( bd \) are integers with \( bd \neq 0 \).
  • Therefore, \( n \) is rational, which contradicts our assumption that \( n \) is irrational.
  • QED
Give a proof by contradiction for “$\sqrt{2}$ is irrational”.
Proof Strategies for proving $p \rightarrow q$

• Choose a method.
  1. First try a direct method of proof.
  2. If this does not work, try an indirect method (e.g., try to prove the contrapositive).

• For whichever method you are trying, choose a strategy.
  1. First try **forward reasoning**. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with $p$ and prove $q$, or start with $\neg q$ and prove $\neg p$.
  2. If this doesn’t work, try **backward reasoning**. When trying to prove $q$, find a statement $p$ that we can prove with the property $p \rightarrow q$. 
Theorems that are Biconditional Statements

- To prove a theorem that is a biconditional statement, i.e., a statement of the form \( p \leftrightarrow q \), we show that \( p \rightarrow q \) and \( q \rightarrow p \) are both true.

- For example, to prove the theorem “if \( n \) is an integer, then \( n \) is odd if and only if \( n^2 \) is odd,” we write:
  “First, we show that if \( n \) is odd then \( n^2 \) is odd.
  --- proof that \( n \) is odd implies \( n^2 \) is odd goes here -----

  Next, we show that if \( n^2 \) is odd, then \( n \) is odd.
  --- proof that \( n^2 \) is odd implies \( n \) is odd goes here -----

  QED”

- Can use different proof methods for each conditional statement.
What is wrong with this?

“Proof” that 1 = 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. $a = b$</td>
<td>Premise</td>
</tr>
<tr>
<td>2. $a^2 = a \times b$</td>
<td>Multiply both sides of (1) by $a$</td>
</tr>
<tr>
<td>3. $a^2 - b^2 = a \times b - b^2$</td>
<td>Subtract $b^2$ from both sides of (2)</td>
</tr>
<tr>
<td>4. $(a - b)(a + b) = b(a - b)$</td>
<td>Algebra on (3)</td>
</tr>
<tr>
<td>5. $a + b = b$</td>
<td>Divide both sides by $a - b$</td>
</tr>
<tr>
<td>6. $2b = b$</td>
<td>Replace $a$ by $b$ in (5) because $a = b$</td>
</tr>
<tr>
<td>7. $2 = 1$</td>
<td>Divide both sides of (6) by $b$</td>
</tr>
</tbody>
</table>
Proof by Cases

• To prove a conditional statement of the form:

\[(p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q\]

• Use the tautology

\[
\left[ (p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q \right] \iff \\
\left[ (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q) \right]
\]

• Each of the implications \( p_i \rightarrow q \) is a case.
Show that $|xy| = |x| |y|$, where $x$ and $y$ are real numbers.
Without Loss of Generality

- Show that if \( x \) and \( y \) are integers and both \( xy \) and \( x+y \) are even, then both \( x \) and \( y \) are even.

- We will use a proof by contraposition.
- What do we assume?

- What do we want to prove?
• Show that if $x$ and $y$ are integers and both $xy$ and $x+y$ are even, then both $x$ and $y$ are even.
Without Loss of Generality

- For the proof of “Show that if $x$ and $y$ are integers and both $xy$ and $x+y$ are even, then both $x$ and $y$ are even.”

We only cover the case where $x$ is odd because the case where $y$ is odd is similar. The phrase *without loss of generality* (w.l.o.g.) indicates this.
A note about writing proofs….

• If you are writing a direct proof, you do not need to write that the proof is a direct proof.

• If you are using a different proof method, it is common to state which proof method you are using at the beginning of the proof, e.g.,
  • “This is a proof by contradiction.”
  • “This is a proof by contraposition.”
  • “This is a proof by induction.”
A note about writing proofs…

• For a proof of $p \rightarrow q$ by contraposition, we write something like…

“This is a proof by contraposition. Assume $\neg q$ is true.

Steps from $\neg q$ to $\neg p$ go here

This implies that $\neg p$ is also true. Therefore, if $p$ is true, then $q$ is true.”

For this class, this sentence is optional
Existence Proofs

• Some theorems are of the form $\exists x P(x)$
  • E.g., “There is a positive integer that can be written as the sum of cubes of two positive integers in two different ways:

• **Constructive existence proof:**
  • Find an explicit value of $c$, for which $P(c)$ is true.
  • Then $\exists x P(x)$ is true by Existential Generalization (EG).

• **Proof:** 1729 is such a number since
  \[ 1729 = 10^3 + 9^3 = 12^3 + 1 \]
Nonconstructive Existence Proofs

• In a nonconstructive existence proof:
  • We prove that a $c$ exists that makes $P(c)$ true, but we don’t actually find what that $c$ is.
  • One option: we assume no $c$ exists for which $P(c)$ is true and derive a contradiction.
Theorem: “There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.”

Proof:

• We know that $\sqrt{2}$ is irrational.
• Consider the number $(\sqrt{2})^{\sqrt{2}}$.
  • If it is rational, we have found two numbers ($x = \sqrt{2}$, $y = \sqrt{2}$) for which $x^y$ is rational.
  • If it is irrational, then let $x = (\sqrt{2})^{\sqrt{2}}$ and let $y = \sqrt{2}$.
  • Then $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  • So, we have found two numbers ($x = (\sqrt{2})^{\sqrt{2}}$ and $y = \sqrt{2}$) for which $x^y$ is rational.

• We proved that there exist such $x$ and $y$, but there are two possibilities for their values. We didn’t say which was the solution.