Topics this week:

- Hour 1 - Proof by Induction (examples 3.4 and 3.5)
- Hour 2 - Worksheets: induction, triangular numbers, inequalities, changing the base case.
- Hour 3 - more induction, proof by contradiction (theorem 2.3), quick introduction to binary representations
- Hour 4 - Worksheets: induction on sets, counting subsets

CSC165 Student Questions / Announcements

- Problem Set 2 is due on Friday. See the extra office hours schedule on the course website.
- Problem Set 1 marks / solutions should be posted sometime early this week.
- See the exam page on the course website for midterm 1 info.

---

Why do you divide into two cases in the proof?

(from Piazza: https://piazza.com/class/k4x63duzocr4gl?cid=354)

Here is a helpful way to think about it: suppose you want to show

\((P \lor Q) \Rightarrow R\)

**Assume** \(P \lor Q\)

Case 1: \(P\) is true

...  

Case 2: \(P\) is false, then \(Q\) must be true by the original assumption.

In this way your cases only directly involve the truth value of \(P\), so you need only consider 2 cases. You could further break down case 1 by the truth value of \(Q\) if need be*.

*But note that Case 1 must work if \(Q\) is true or if \(Q\) is false.
How do I know when to expand a definition?

If you have external facts to use, look at what form they are in. For example, in the proof last week the external facts contained $n \nmid m$, so that suggested we didn’t need to expand the definition of our assumption $n \nmid a$.

Go to menti.com and enter the code 99 95 73

CSC 165 Lecture 9

Proof by Induction (Chapter 3 in course notes)

Quick recap of simple induction from prep reading

Proof Template:

Prove that $\forall n \in \mathbb{N}, P(n)$.

Proof:

1. Base case:

   [Prove $P(0)$]

2. Inductive step:

   Let $k \in \mathbb{N}$. Assume $P(k)$

   [Prove $P(k+1)$]
Simplified version of Example 3.4 (page 68)

\[
\forall x, y \in \mathbb{Z}, \forall n \in \mathbb{N}, 5 \mid x - y \Rightarrow 5 \mid x^n - y^n
\]

**Proof:** Let \( x, y \in \mathbb{Z} \). We'll prove, by induction, that \( \forall n \in \mathbb{N}, 5 \mid x - y \Rightarrow 5 \mid x^n - y^n \).

**Base case:** Let \( n = 0 \). Assume \( 5 \mid x - y \) and prove \( 5 \mid x^0 - y^0 \):

\[
5 \mid x^0 - y^0
\]

\[
5 \mid 0
\]

**Inductive step:** Let \( k \in \mathbb{N} \). Assume \( 5 \mid x - y \Rightarrow 5 \mid x^k - y^k \).

Show that \( 5 \mid x - y \Rightarrow 5 \mid x^{k+1} - y^{k+1} \).

**Base:** Assume \( 5 \mid x^k - y^k \), then show \( 5 \mid x^{k+1} - y^{k+1} \).

**Body:** Start with \( x^{k+1} - y^{k+1} = x^{k+1} - x^k y + y^{k+1} 

\[
= x^{k+1} (x - y) + y^{k+1} (x - y)
\]

**End:** Assume \( a, b, x, y \in \mathbb{Z} \), \( 5 \mid x \land 5 \mid y \Rightarrow 5 \mid ax + by \). 

\[\hline\]
From (2) and I.H, we conclude that $5 \mid x^k - y^k$

$5 \mid x - y$

So by Ex.1, we have that $5 \mid x^{k+1} - y^{k+1}$.

Example 3.5 (bottom of page 69 and page 70)

Prove $\forall n \in \mathbb{N}, n \geq 3 \implies 2n+1 < 2^n$

$\forall n \in \mathbb{N}, P(n)$
Proof: Let \( n = 3 \).

Prove \( 2n+1 < 2^n \).

\[
2(3) + 1 < 2^3 \\
7 < 8.
\]

Inductive step. Let \( k \in \mathbb{N} \), assume \( k \geq 3 \).

Assume \( 2k+1 < 2^k \) (I.H.).

Prove that \( 2(k+1)+1 < 2^{k+1} \).

We start with \( 2(k+1)+1 \)

\[
= 2k + 2 + 1 \\
= 2k + 1 + 2 \\
= 2k + 2 \\
= 2^k + 2 \quad \text{(by I.H.)}
\]

Since \( k \geq 3 \) by assumption, so

\[
2^k \geq 2^3 = 8 > 2
\]
\[2^{(k+1)} + 1 < 2^k + 2 \leq 2^{k+2} \]
CSC165 Student Questions / Announcements

- Pset2 due Friday (see course website for extra office hours)
- Midterm next week (see Exam page for information - note the exact time and location)
- Are the CSC240 resources public for anyone interested in reading ahead? 

- If you have P(x,y) can you prove P(x,y) is true for all pairs of natural numbers with induction? 
  You can, but it is more work than simple induction - see for example:
  Discrete Math with Proof (Gossett)
  Textbook section 3.5.5 (page 148) Multidimensional induction
  related: 236 and 240 will cover structural induction

- Advice for writing proofs?
  See the course notes and review the templates for each type of proof.

  Go to menti.com and enter the code 99 95 73
  (if you have questions during lecture)
CSC 165 Lecture 10

An incorrect induction proof, proof by contradiction, binary representations

Incorrect proofs by induction (page 75)

"All jelly beans have the same colour"

\[ P(n) : \text{"any set of } n \text{ jelly beans, every jelly bean has the same colour"} \]

**Base Case:**

\[ P(1) : \text{one jelly bean has one colour} \]

**Induction Step:** Assume \( P(k) \), show \( P(k+1) \).

Let \( S = \{ j_1, j_2, \ldots, j_k, j_{k+1} \} \) be a set of \( k+1 \) jelly beans.

Let \( S_1 = \{ j_1, j_2, \ldots, j_k \} \). By IH, if \( j \in S_1 \) then \( j \) has the same colour as \( j_1 \).

Let \( S_2 = \{ j_2, j_3, \ldots, j_k, j_{k+1} \} \). By IH, \( j_{k+1} \) has the same colour as \( j_1 \).

\[ S_1 \cap S_2 \neq \emptyset \text{, so } c_1 = c_2 \]

What if \( \delta = 1 \)?

\[ \delta + 1 = 2 \]
Theorem 2.3 There are infinitely many primes.

Proof (by contradiction):

Assume finitely many primes. Let \( k \in \mathbb{N} \) be the number of primes. Let \( \mathcal{P} = \{p_1, p_2, \ldots, p_k\} \) be the set of all primes.

Let \( Q \) be \( \forall q, p, q \in \mathbb{Z}, p < q \Rightarrow p \mid q + a p \).

\[
\begin{align*}
\neg p &\Rightarrow (Q \land \neg Q) \\
\neg p &\Rightarrow (Q \land \neg Q) \\
\neg p &\Rightarrow (Q \land \neg Q) \quad \text{free to choose } Q.
\end{align*}
\]
- \( Q: \exists a, p, q \in \mathbb{Z}, p | q \land p \neq q + a \)

Show \(-Q\).

Let \( q = 1 + \prod_{i=1}^{k} p_i \)

\[ q = 1 + p_1 \cdot p_2 \cdot \ldots \cdot p_k \]

Because \( q \geq 1 \), we know there exists some \( p \) such that \( \text{Prime}(p) \land p | q \)

Let \( a = \frac{1}{p} \prod_{i=1}^{k} p_i \)

\[ a + p | \prod_{i=1}^{k} p_i \]

\[ 1 + \prod_{i=1}^{k} p_i - \frac{p}{p} \prod_{i=1}^{k} p_i = 1 \]

\( p \neq 1 \)

Conclude \( p \) is true.
Textbook: A.

Q: \( \forall n \in \mathbb{N}, \text{Prime}(n) \iff (n \in \mathbb{P}) \)

\[-Q \iff \exists n \in \mathbb{N}, \text{Prime}(n) \land n \notin \mathbb{P} \]

the \( \mathbb{P} \) we defined is not an

\[ \forall n. \]

Binary Representation of Numbers (we’ll just introduce the definitions now and then talk more about them next week)

Let \( m \in \mathbb{N} \). A binary representation of \( m \) is a number \( k \in \mathbb{Z}^+ \) and bits \( b_0, b_1, \ldots, b_{k-1} \in \{0, 1\} \) such that

\[
m = \sum_{i=0}^{k-1} b_i \times 2^i
\]

Example:

\[
4 = (100)_2
\]

\[
4 = (0100)_2
\]

\[ k = 4, \]

\[
4 = (b_{k-1} \ldots b_1 b_0)_2
\]
What is \((10100101)_2\) in decimal? 

\[
\begin{align*}
1 \times 2^0 + 1 \times 2^2 + 1 \times 2^5 + 1 \times 2^7 &= \underline{165} \\
\end{align*}
\]

\[
\sum_{i=0}^{7} \begin{cases} 1 & \text{if } a_i = 1 \\ 0 & \text{otherwise} \end{cases} \times 2^i
\]