Topics this week:

- Hour 1 - a proof about primes / divisibility, remarks about proof body, a generalization example (odd * odd = odd)
- Hour 2 - Worksheets: gcd, proof by cases, indirect proof / contrapositive
- Hour 3 - Example of a proof (Example 2.15 / 2.16) [contrapositive, converse, characterization]
- Hour 4 - Worksheets: proofs about primes / gcd, using external facts in proofs

CSC165 Student Questions / Announcements

- If you are looking for a group for the problem sets or someone to work on the worksheets with in class, consider making a post on Piazza - or ask someone in class if they want to work together.
- **Problem Set 2 is out. Please read through all the questions and start thinking about the proofs. It often takes time to figure things out, so start early.**

Is it necessary to write header and body in the proof?

- No

We don’t get to choose a value for k1?

- In the proof from last class, the key is that we **assume** that there exists a k1 such that x + 5 = k1 x. Once we have assumed such a k1 exists, we can use it like any other variable.

Go to [menti.com](https://menti.com) and enter the code 99 95 73
More about proofs

Recall definitions of prime / statement proven last class:

\[ \text{Prime}(p) : p > 1 \land (\forall d \in \mathbb{N}, d|p \implies d=1 \lor d=p) \]

\[ \forall d, x \in \mathbb{Z}, x \mid x + d \implies x \mid d \]

Example: Prove that for all natural numbers \( x \) and \( p \), if \( p \) is prime and \( x \mid x + p \), then \( x = 1 \) or \( x = p \).

Translation:

\[ \forall x, p \in \mathbb{N}, \text{Prime}(p) \land x \mid x + p \implies x = 1 \lor x = p. \]

Proof:

Let \( x, p \in \mathbb{N} \).
Assume that $p$ is prime and that $x \mid x + p$. We want to prove that $x \leq 1$ or $x = p$. Since we assumed $x \mid x + p$, we can state

\[ x \mid x + p \]

to conclude that $x \mid p$. By previous deduction, since we also assumed that $p$ is prime, so by definition: $\forall d \in \mathbb{N}, d \mid p \Rightarrow d = 1 \vee d = p$. So then using this definition, since $x \mid p$, we conclude that $x \leq 1$ or $x = p$. □

Remarks about proof bodies (page 42 in course notes)
Generalization example:

How to generalize "for all ints a, b if 2 does not divide a and 2 does not divide b then 2 does not divide ab"? (odd * odd = odd)

Let's generalize the statement:

\[ \forall d \in \mathbb{Z}, \exists x \in \mathbb{Z} : d | x \text{ and } 2 | x \implies 2 | x \cdot 5 \]

\[ \forall a, b \in \mathbb{Z}, 2 \nmid a \land 2 \nmid b \implies 2 \nmid ab \]

\[ \forall d \in \mathbb{Z}, \forall a, b \in \mathbb{Z} : d \nmid a \land d \nmid b \implies d \nmid ab ? \]

Let's consider the counterexample:

\[ d = 4, a = 2, 4 \nmid 2 \]

\[ b = 2, 4 \nmid 2 \times 2 \]

\[ 414 \]
CSC165 Student Questions / Announcements

• If you are looking for a group for the problem sets, see the pinned Search for Teammates! note on Piazza

Problem Set 2 is out. Please read through all the questions and start thinking about the proofs. It often takes time to figure things out, so start early.

• Midterm 1

  • on Monday February 10
  • Students must write in the section they're enrolled in, and can check the exact time and location for their section on the "Exams" page of the course website.
  • There are a limited number of spots to accommodate students writing with a different section; they should email the course email address to request to write with a different section.
  • We've posted some more information about the midterm, and some past tests, on the course website (under the "Exams" page).

Preparing for the midterm:
• For a given question, identify which **concepts** in this course are relevant to the question.
• For a given question, come up with multiple ways of solving it (rather than just one).
• Teach a course concept or explain a solution to someone else.
• Create some new questions (with friends!) and then solve them.

**CSC 165 Lecture 8**

More proofs (examples 2.15 and 2.16)

Continuation of example from the end of last class - proof using the **contrapositive** and then we will consider the **converse** of the statement and prove that too (example of proving an if and only if statement)

\[
\forall n \in \mathbb{N}, \left( (\forall a, b \in \mathbb{N}, n \nmid a \land n \nmid b \Rightarrow n \nmid ab) \land n > 1 \right) \Rightarrow \text{Prime}(n)
\]

Characterization:

an alternate definition

\[
\text{Prime}(n) : n > 1 \land \left( \forall d \in \mathbb{N} \quad d | n \Rightarrow d = 1 \lor d = n \right)
\]

"different way to look at things"

( the same thing / concept)
Setting up the header for the proof (proof body left as a worksheet exercise)

\[ \rho \Rightarrow q \]

**Contrapositive:** \( \neg q \Rightarrow \neg \rho \)

\( \forall \alpha \in \mathbb{N}, \neg \text{Prime}(\alpha) \Rightarrow (\exists a, b \in \mathbb{N}, \alpha \nmid a \land \alpha \nmid b \land \alpha \nmid ab) \land \alpha \leq 1 \lor \alpha \not\mid n \)

**Proof:** Let \( n \in \mathbb{N} \).

Assume \( n \) is not prime,

\( \neg \text{Prime}(n) \)

\( \exists h \leq 1 \lor \exists x \in \mathbb{N}, x \mid n \land x \neq 1 \land x \neq n \)

**Case 1:** Assume \( n \leq 1 \):

The second part of the OR that we want to prove is \( \text{True}(n \leq 1) \).

**Case 2:** Assume \( \exists x \in \mathbb{N}, x \mid n \) and \( x \neq 1 \) and \( x \neq n \)

From the first assumption above,

\( \exists k \in \mathbb{Z}, kx = n \).

Let \( a = k \). Let \( b = x \).

We want to prove that \( n \nmid a, n \nmid b, \) and \( n \nmid ab \).
Short Break: Go to menti.com and enter the code 99 95 73

Proving the converse (example 2.16):

\[ \forall n \in \mathbb{N}, \text{Prime}(n) \Rightarrow ((\forall a, b \in \mathbb{N}, n \nmid a \land n \nmid b \Rightarrow n \nmid ab) \land n > 1) \]

Proof: Let \( n \in \mathbb{N} \) and assume \( n \) is prime.

Part 1: Prove that \( n > 1 \).

True by definition of \( \text{Prime}(n) \).

Part 2: Prove that \( \forall a, b \in \mathbb{N}, n \nmid a \land n \nmid b \Rightarrow n \nmid ab \)

Let \( a, b \in \mathbb{N} \). Assume \( n \nmid a \land n \nmid b \).

We want to prove that \( n \nmid ab \).

1. \( \forall n, m \in \mathbb{N}, \text{Prime}(n) \land n \nmid m \Rightarrow (\exists r, s \in \mathbb{Z}, rm + sn = 1) \)

Some “helper” facts about primes to help with our proof:

2. \( \forall n, m \in \mathbb{N}, \text{Prime}(n) \land (\exists r, s \in \mathbb{Z}, n \times 5m = 1) \)
Rough Work:

Assumptions: \( \text{Prime}(n) \)

1. \( n+a \)
2. \( n+b \)

Using:
1. \( \exists r_1, s_1 \in \mathbb{Z}, \quad r_1 n + s_1 a = 1 \) \( A \)
2. \( \exists r_2, s_2 \in \mathbb{Z}, \quad r_2 n + s_2 b = 1 \) \( A \)

\( b, s_2 \rightarrow r_2 n + s_2 (ab) \equiv 1 \)

Using:
2. \( \text{Prime}(n) \land \left( \forall r, s \in \mathbb{Z}, \quad r n + s ab = 1 \right) \Rightarrow n \not\mid ab \)