Week 3 - Friday

COMP 2230

Last time

- Rational numbers
- Divisibility

Questions?

Assignment 1

Logical warmup

- Two women are sitting in a street cafe, talking about their children.
- One says she has three daughters. The product of their ages is 36, and the sum of their ages is the number of the house across the street.
- The second woman replies that this information is not enough to figure out the age of each child.
- The first agrees and adds that her oldest daughter has beautiful blue eyes.
- Then the second solves the puzzle.
- What are the ages of the daughters?

Divisibility

Unique factorization theorem

- For any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$$

- And any other expression of n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written

Proof by Cases

Proof by cases

- If you have a premise consisting of clauses that are ANDed together, you can split them up
    - Each clause can be used in your proof
- What if clauses are ORed together?
- You don't know for sure that they're all true
- In this situation, you use a proof by cases
- Assume each of the individual possibilities is true separately
- If the proof works out in all possible cases, it still holds

Proof by cases formatting

- For a direct proof using cases, follow the same format that you normally would
- When you reach your cases, number them clearly
- Show that you have proved the conclusion for each case
- Finally, after your cases, state that, since you have shown the conclusion is true for all possible cases, the conclusion must be true in general

Quotient-remainder theorem

- For any integer n and any positive integer d, there exist unique integers q and r such that
  - $n = dq + r$ and $0 \leq r < d$
- This is a fancy way of saying that you can divide an integer by another integer and get a unique **quotient** and **remainder**
- We will use **div** to mean integer division (exactly like **/** in Java)
- We will use **mod** to mean integer mod (exactly like **%** in Java)
- What are q and r when $n = 54$ and $d = 4$?

Consecutive integers have opposite parity

- Prove that, given any two consecutive integers, one is even and the other is odd
- **Hint:** Divide into two cases:
  - The smaller of the two integers is even
  - The smaller of the two integers is odd

Another proof by cases

- Theorem: for all integers n, $3n^2 + n + 14$ is even
- How could we prove this using cases?
- Be careful with formatting

Indirect Proof

Proof by contradiction

- The most common form of indirect proof is a proof by contradiction
- In such a proof, you begin by assuming the negation of the conclusion
- Then, you show that doing so leads to a logical impossibility
- Thus, the assumption must be false and the conclusion true

Contradiction formatting

- A proof by contradiction is different from a direct proof because you are **trying** to get to a point where things don't make sense
- You should always mark such proofs clearly
- Start your proof with the words **Proof by contradiction**
- Write **Negation of conclusion** as the justification for the negated conclusion
- Clearly mark the line when you have both p and $\sim p$ as a **contradiction**
- Finally, state the conclusion with its justification as the contradiction found before

Example

- **Theorem:** There is no largest integer.
- **Proof by contradiction:** Assume that there is a largest integer.

Another example

- **Theorem:** There is no integer that is both even and odd.
- **Proof by contradiction:** Assume that there is an integer that is both even and odd

Another example

- **Theorem:** $\forall x, y \in \mathbb{Z}^{+}, x^2 - y^2 \neq 1$
- **Proof by contradiction:** Assume there is such a pair of integers

Two Classic Results

Square root of 2 is irrational

Theorem: $\sqrt{2}$ is irrational

Proof by contradiction:

1.	Suppose $\sqrt{2}$ is rational	1.	Negation of conclusion
2.	$\sqrt{2} = m/n$, where $m, n \in \mathbb{Z}, n \neq 0$ and m and n have no common factors	2.	Definition of rational
3.	$2 = m^2/n^2$	3.	Squaring both sides
4.	$2n^2 = m^2$	4.	Transitivity
5.	$2k = m^2, k \in \mathbb{Z}$	5.	Square of integer is integer
6.	$m = 2a, a \in \mathbb{Z}$	6.	Even x^2 implies even x (Proposition 4.7.4)
7.	$2n^2 = (2a)2 = 4a^2$	7.	Substitution
8.	$n^2 = 2a^2$	8.	Transitivity
9.	$n = 2b, b \in \mathbb{Z}$	9.	Even x^2 implies even x
10.	$2\|m$ and 2|n	10.	Conjunction of 6 and 9, **contradiction**
11.	$\sqrt{2}$ is irrational	11.	By contradiction in 10, supposition is false

■

Proposition 4.7.3

Claim: $\forall a, p \in \mathbb{Z}\ \ p$ is prime $\wedge\, p \mid a \rightarrow p \nmid a + 1$
Proof by contradiction:

1.	Suppose $\exists a, p \in \mathbb{Z}$ such that p is prime $\wedge\, p \mid a \wedge p \mid a + 1$	1.	Negation of conclusion
2.	$a = p \cdot r, r \in \mathbb{Z}$	2.	Definition of divides
3.	$a + 1 = p \cdot s, s \in \mathbb{Z}$	3.	Definition of divides
4.	$(a + 1) - a = 1$	4.	Subtraction
5.	$p \cdot s - p \cdot r = 1$	5.	Substitution
6.	$p(s - r) = 1$	6.	Distributive law
7.	$p \mid 1$	7.	Definition of divides
8.	$p \leq 1$	8.	Since 1 and -1 are the only integers that divide 1
9.	$p > 1$	9.	Definition of prime
10.	Contradiction	10.	Statements 8 and 9 are negations of each other
11.	$\forall a, p \in \mathbb{Z}\ \ p$ is prime $\wedge\, p \mid a \rightarrow p \nmid a + 1$	11.	By contradiction at statement 10

■

Infinitude of primes

Theorem: There are an infinite number of primes

Proof by contradiction:

1.	Suppose there is a finite list of all primes: $p_1, p_2, p_3, \ldots, p_n$	1.	Negation of conclusion
2.	Let $N = p_1 p_2 p_3 \ldots p_n + 1, N$ □ $\mathbb{Z}$	2.	Product and sum of integers is an integer
3.	$p_k \mid N$ where p_k is a prime	3.	Theorem 4.4.4
4.	$p_k \mid p_1 p_2 p_3 \ldots p_n + 1$	4.	Substitution
5.	$p_1 p_2 p_3 \ldots p_n = p_k (p_1 p_2 p_3 \ldots p_{k-1} p_{k+1} \ldots p_n)$	5.	Commutativity
6.	$p_1 p_2 p_3 \ldots p_n = p_k P, P$ □ $\mathbb{Z}$	6.	Product of integers is integer
7.	$p_k \mid p_1 p_2 p_3 \ldots p_n$	7.	Definition of divides
8.	p_k does not divide $p_1 p_2 p_3 \ldots p_n + 1$	8.	Proposition from last slide
9.	p_k does and does not divide $p_1 p_2 p_3 \ldots p_n + 1$	9.	Conjunction of 4 and 8, **contradiction**
10.	There are an infinite number of primes	10.	By contradiction in 9, supposition is false

■

A few notes about indirect proof

- Don't combine direct proofs and indirect proofs
- You're either looking for a contradiction or not
- Proving the contrapositive directly is equivalent to a proof by contradiction

Upcoming

Next time…

- Exam 1!

Reminders

- **Finish Assignment 1**
  - **Due tonight by midnight!**
- Review for Exam 1
  - Next Monday!