Week 3 - Wednesday

COMP 2230

Last time

- Arguments with quantifiers
- Proving existential statements and disproving universal ones
- Proving universal statements

Questions?

Assignment 1

Logical warmup

- Fermat's Last Theorem states that **no** three positive integers a, b, and c satisfy this equation when $n > 2$:
  - $a^n + b^n = c^n$

- A noted computer scientist claims he found a solution where:
  - $a = 2233445566$
  - $b = 7788990011$
  - $c = 9988776655$

- Just as he's about to announce n publicly, a 10-year old boy raises his hand and says that the scientist made a mistake
- How did the boy figure out the scientist was wrong?

Rational Numbers

Another important definition

- A real number is **rational** if and only if it can be expressed at the quotient of two integers with a nonzero denominator
- Or, more formally,

r is rational $\Leftrightarrow \exists\ a, b \in \mathbb{Z},\ r = \frac{a}{b}$ and $b \neq 0$

Prove the following:

- Every integer is a rational number
- The sum of any two rational numbers is rational
- The product of any two rational numbers is a rational number

Prove or disprove:

- The reciprocal of any rational number is a rational number

Using existing theorems

- Math moves forward not by people proving things purely from definitions but also by using existing theorems
- "Standing on the shoulders of giants"
- Given the following:
  1. The sum, product, and difference of any two even integers is even
  2. The sum and difference of any two odd integers are even
  3. The product of any two odd integers is odd
  4. The product of any even integer and any odd integer is even
  5. The sum of any odd integer and any even integer is odd
- Using these theorems, prove that, if a is any even integer and b is any odd integer, then $(a^2 + b^2 + 1)/2$ is an integer

Divisibility

Definition of divisibility

- If n and d are integers, then n is divisible by d if and only if $n = dk$ for some integer k
- Or, more formally:
- For $n, d \in \mathbb{Z}$,
  - n is divisible by $d \Leftrightarrow \exists k \in \mathbb{Z},\ n = dk$
- We also say:
  - n is a multiple of d
  - d is a factor of n
  - d is a divisor of n
  - d divides n
- We use the notation $d \mid n$ to mean "d divides n"

Transitivity of divisibility

- Prove that for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$
- Steps:
  - Rewrite the claim in formal notation
  - Write **Proof:**
  - State your premises
  - Justify every line you infer from the premises
  - Write ■ or QED after you have demonstrated the conclusion

Prove or disprove:

- For all integers a and b, if $a \mid b$ and $b \mid a$, then $a = b$
- How could we change this statement so that it is true?
- Then, how could we prove it?

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

An application of the unique factorization theorem

- Let m be an integer such that
  - $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10$
- Does $17 \mid m$?
- Leave aside for the moment that we could actually compute m

Floor and Ceiling

More definitions

- For any real number x, the floor of x, written $\lfloor x \rfloor$, is defined as follows:
  - $\lfloor x \rfloor$ = the unique integer n such that $n \leq x < n + 1$
- For any real number x, the ceiling of x, written $\lceil x \rceil$, is defined as follows:
  - $\lceil x \rceil$ = the unique integer n such that $n - 1 < x \leq n$

Proofs with floor and ceiling

- Prove or disprove:
  - $\forall x, y \in \mathbb{R}, \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$
- Prove or disprove:
  - $\forall x \in \mathbb{R}, \forall m \in \mathbb{Z} \; \lfloor x + m \rfloor = \lfloor x \rfloor + m$

Ticket Out the Door

Upcoming

Next time…

- Proofs by contradiction

Reminders

- Read Sections 4.6, 4.7, and 4.8
- Finish Assignment 1
  - Due Friday!
- Review for Exam 1
  - Next Monday!