Week 4: Elementary Number Theory and Methods of Proof

Agenda:

- Direct Proof and Counterexample
  - Direct proof and counter-example
  - indirect arguments: contradiction and contraposition

Reading:

- Textbook pages 125–178.

Firt we will see one more example about the relational database system of a library we were discussing last week. Let's consider the following query:

"Find the names of all subscribers who have borrowed all books written by "Williams" from the library".

- A little bit of thinking convinces one that this is ambigious. It can be interpreted as either of the following two:
  - Find the names of all subscribers who have borrowed every single copy of every book written by "Williams", or
  - Find the names of all subscribers who have borrowed at least one copy of every book written by Williams that the library has

- The predicate formula corresponding to the first interpretation is the following:

  $\exists s \exists a(\texttt{Subscriber}(s,n,a) \wedge \forall b(\exists t \texttt{Book}(b,t,'Williams') \rightarrow \exists d \texttt{Borrowed}(s,b,d))))$

  This can be rephrased as follows:
  Find all names n' that can be substituted for n s.t. there is a subscriber named n' who has some SIN s and lives at some addresss a, and for every book id b, if b is written by "Williams" and has some title t, then subscriber s has borrowed b for some return date.

- For the second interpretation we have the following:

  $\exists s \exists a(\texttt{Subscriber}(s,n,a) \wedge \forall t(\exists b \texttt{Book}(b,t,''Williams'')$
  $\rightarrow \exists b'(\texttt{Book}(b',t,''Williams'') \wedge \exists d \texttt{Borrowed}(s,b',d)))))$

  Rephrase: find all names n' that can be substitued for the variable n s.t. there is a subscriber called n' who has some SIN s and lives at some address a and, for very title t, if there is a book (with some id b) with title t written by Williams, then there is a book also with title t and written by Williams with possibly a different id b' which subscriber s has borrowed (and must be returned by some due date d).

In mathematics:

- **Definitions** are often **biconditional**, e.g.,
  - An **even** integer is one that equals twice some integer.

    n is even $\Leftrightarrow \exists$ an integer k such than $n = 2k$
  - n is **odd** $\Leftrightarrow \exists$ an integer k such than $n = 2k + 1$
  - $n > 1$ is **prime** $\Leftrightarrow \forall$ positive integers r and s, if $n = r \cdot s$ then $r = 1$ or $s = 1$
  - $n > 1$ is **composite** $\Leftrightarrow \exists$ positive integers r and s such that $n = r \cdot s$ and $r \neq 1$ and $s \neq 1$
- **Theorems** are (mathematical) statements that are known/proved to be true.
- Proof methods:
  - Direct proof
  - Proof by contraposition
  - Proof by contradiction

Proving Existential Statements:

- General form of $\exists x \in D, P(x)$, find a value for x from the domain D that makes $P(x)$ true.
- You can find that value in any way you want (guess, try different values, etc), or (better) you can give directions as to find one (constructive proof).
- Example:
  Prove that: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

Proof: Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$. (**constructive proofs of existence**)

- Example:
  Prove that there is an integer $x > 5$ such that $x^2 - 4x - 12 = 0$.

  Proof: We know that $x^2 - 4x - 12 = (x + 2)(x - 6)$; this implies that for $x = 6$: $x^2 - 4x - 12$ will be zero.

Disproving Universal statements:

- To disprove a statement of the form $\forall x \in D, P(x)$ it is enough to find one value for x from D which makes $P(x)$ false. That is called a *counter-example*.

- Example:
  Disprove that: $\forall$ real numbers a and b, if $a^2 = b^2$ then $a = b$.

  Proof: Let $a = 2$ and $b = -2$. Then $2^2 = (-2)^2$, but $2 \neq -2$.

Proving Universal Statements:

- More important and less trivial proofs involve these type of statements.

- Method of exhaustion: try all possible values from the domain.

  Example:

  Prove that: $\forall n \in \mathcal{Z}$, if n is even and $4 \leq n \leq 10$, then n can be written as a sum of two prime numbers.

  Proof. (**Exhaustion**)

  Not common/effection. Cannot be used if the domain is very large or infinite.

- Direct proof: Show that the statement is true for any arbitrary value of x chosen from the domain

- Definiton: A number r is **rational** $\Leftrightarrow \exists$ integers a and b such that $b \neq 0$ and $r = \frac{a}{b}$

- **Theore:** The sum of any two rational numbers is rational.

  Proof:

  - Suppose r and s are two rational numbers (they are arbitrarily chosen).
  - Then, by definition, $\exists a, b, c, d$ integers such that $b \neq 0$, $d \neq 0$, and $r = \frac{a}{b}$ and $s = \frac{c}{d}$.
  - Therefore,
  $$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$
  - Let $p = ad + bc$ and $q = bd$.
  - Then, p, q are integers and $q \neq 0$.
  - It follows that $r + s$ is rational.

- General steps in such a proof:
  - Make sure the statement to be proved is written down clearly.
  - Mark clearly the beginning of the proof (using word "Proof").
  - Make the proof self-contained.
  - explain non-trivial steps: "note that ...", "This is because....", "Follows from .... and ...."

Disproving Existential Statements

- To disprove a statement of the form $\exists x \in D, P(x)$ we have to prove that $\forall x, \sim P(x)$.

- Example:

  Prove or disprove that there is an integer $x \geq 1$ s.t. $x^2 + 3x + 2$ is prime.

  We will disprove this. We show that for all integers $x \geq 1$, x^2+3x+2 is composite. Note that $x^2 + 3x + 2 = (x + 1)(x + 2)$. For every integer $x \geq 1$ we have: $x + 1 \geq 2$ and $x + 2 \geq 2$. Thus $x^2 + 3x + 2$ can be written as product of two numbers each of which is at least 2, so it is not prime.

Divisibility:

- n and $d \neq 0$ are integers:

  n is **divisible** by d if and only if $n = dk$ for some integer k.

- Equivalently,
  - n is a multiple of d
  - d is a factor of n
  - d is a divisor of n
  - d divides n
  - $d \mid n$

- Some trivial properties:
  - $d \mid 0$
  - $d \mid d$
  - $1 \mid n$

Properties of divisibility:

- An integer $n > 1$ is **prime** if and only if its only positive integer divisors are 1 and itself.

- **Transitivity**: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

  Proof: Suppose that a, b, c are arbitrary integers such that $a \mid b$ and $b \mid c$. So there exists integers r, s s.t. $b = ar$ and $c = bs$. This implies that $c = (ar)s = a(rs)$. Since r and s are integers, so is $k = rs$. Thus $c = ak$ for some integer k and thus $a \mid c$.

- **Divisibility by a Prime**: any integer $n > 1$ is divisible by a prime number.

  Proof. (as in the textbook).

- **Fundamental Theorem of Arithmetic**: given 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

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

  and this expression of n as a product of prime numbers (**standard factored form**) is **unique**.

- **Quotient-Remainder Theorem**: given any integer n and positive integer d, there exist unique integers q and r such that

  $$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

- e.g. any integer n can be expressed as $n = 2q + 0$ or $n = 2q + 1$ (but not both).

- This means any integer n is either even or odd (but not both)

- Prove that, the square of any odd integer has the form $8m + 1$ for some integer m

  Proof: Let n be an odd number. Then, $n = 4q + 1$ or $n = 4q + 3$, for some q.

  - Case 1 ($n = 4q + 1$):
    $n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1$
    Let $m = 2q^2 + q$; so m is an integer since q is an integer.

Then, $n^2 = 8m + 1$, as wanted.

- Case 2 ($n = 4q + 3$):
  $n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1$
  Let $m = 2q^2 + 3q + 1$; again m is an integer since q is.
  Then, $n^2 = 8m + 1$, as wanted.

so in both cases, n^2 has the form $8m + 1$ for some integer m.

Floor and Ceiling:

- Given any real number x, the **floor** of x, $\lfloor x \rfloor$, is defined as

$$\lfloor x \rfloor = n, \quad \text{such that } n \leq x < n + 1.$$

- The **ceiling** of x, $\lceil x \rceil$, is defined as

$$\lceil x \rceil = n, \quad \text{such that } n - 1 < x \leq n.$$

- Example $\lfloor 4.3 \rfloor = 4$, $\lfloor 0.82 \rfloor = 0$, $\lfloor -2.2 \rfloor = -3$, $\lceil -0.92 \rceil = 0$, $\lceil 3 \rceil = 3$.

- **Theorem:** $\forall x \in \mathbb{R}$ and $\forall m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

  Proof:
  Let $x \in \mathbb{R}$ be an arbitrary real and $m \in \mathbb{Z}$ be an arbitrary integer. By definition, there is an integer n, s.t. $n \leq x < n + 1$ i.e. $\lfloor x \rfloor = n$.

  Add m to all sides, we get: $n + m \leq x + m < n + m + 1$, i.e. $\lfloor x + m = n + m = \lfloor x \rfloor + m$.

- True or False?
  - $\forall x, y \in RR$: $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$
    Flase, e.g. let $x = 1.5$ and $y = 1.5$.
  - $\lfloor 2x \rfloor = 2\lfloor x \rfloor$
    False, e.g. let $x = 1.1$.

Proof by contradiction:

- General steps:
  1. Suppose the statement to be proved is false.
     That is, suppose that the negation of the statement is true.
  2. Show that this supposition leads logically to a contradiction.
  3. Conclude that the statement to be proved is true.

- Example:

  Theorem: Sum of any rational and any irrational number is irrational.

  Proof: By way of contradiction, suppose there is a rational number r and irrational number s s.t. $r + s$ is rational.

  By definition, there are integers a, b, c, d s.t. $b \neq 0$, $d \neq 0$, and $r = \frac{a}{b}$ and $r + s = \frac{c}{d}$.

  So $\frac{a}{b} + s = \frac{c}{d}$ which implies $s = \frac{c}{d} - \frac{a}{b} = \frac{cb-ad}{bd}$.

  Since b, d are non-zero, so is bd. Also, both $cb - ad$ and bd are integers, so s is rational, which contradicts the assumption.

Proof by contraposition:

- General steps:
  1. Rewrite the statement in the contrapositive form.
  2. Prove the contraposition by a direct proof.
  3. Conclude from the equivalence that the statement to be proved is true.

- Example:
  Theorem For all integers n, if n^2 is even then n is even.

  Proof: We prove that for all integers n if n is odd then n^2 is odd. This is the contrapositive of the original statement and therefore is equivalent to it.

Let n be any odd integer. So it has the form $n = 2q + 1$ for some integer q.

Therefore, $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1$. Let $k = 2q^2 + 2q$; so k is an integer and thus $n^2 = 2k + 1$ for some integer; so it is odd.