Elementary Number Theory and Methods of Proof (I)

Lecture 07 / Spring 2015
State University of New York, Korea
Instructor: Dr. Ilchul Yoon

Adapted from slides by Paul Fodor

Number theory

- Properties of integers (whole numbers), rational numbers (integer fractions), and real numbers.
- Truth of mathematical statements.
- Example:
  - Definition: For any real number $x$, the floor of $x$, $\lfloor x \rfloor$, is the largest integer that is less than or equal to $x$
    
    $[2.3] = 2; \quad [12.99999] = 12; \quad [-1.5] = -2$
  - Properties:
    - For any real number $x$, is $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$?
      * yes (true)
    - For any real numbers $x$ and $y$, is $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$?
      * no (false)
        - $\lfloor 2.0 - 1.1 \rfloor = [0.9] = 0$
        - $\lfloor 2.0 \rfloor - \lfloor 1.1 \rfloor = 2 - 1 = 1$
Number theory

- Proof example:
  - If $x$ is a number with $5x + 3 = 33$, then $x = 6$

  **Proof:**
  
  If $5x + 3 = 33$, then $5x + 3 - 3 = 33 - 3$ since subtracting the same number from two equal quantities gives equal results.
  
  $5x + 3 - 3 = 5x$ because adding 3 to $5x$ and then subtracting 3 just leaves $5x$, and also, $33 - 3 = 30$.
  
  Hence $5x = 30$.
  
  That is, $x$ is a number which when multiplied by 5 equals 30.
  
  The only number with this property is 6.
  
  Therefore, if $5x + 3 = 33$ then $x = 6$.

Number theory introduction

- Properties of equality:
  
  (1) $A = A$
  
  (2) if $A = B$ then $B = A$
  
  (3) if $A = B$ and $B = C$, then $A = C$

- The set of all integers is closed under addition, subtraction, and multiplication.
Number theory introduction

- An integer n is **even** if, and only if, n equals twice some integer:
  \[ n \text{ is even } \iff \exists \text{ an integer } k \text{ such that } n = 2k \]

- An integer n is **odd** if, and only if, n equals twice some integer plus 1:
  \[ n \text{ is odd } \iff \exists \text{ an integer } k \text{ such that } n = 2k + 1 \]

- Reasoning examples:
  - Is 0 even?
    - Yes, \( 0 = 2 \cdot 0 \)
  - Is −301 odd?
    - Yes, \( −301 = 2(−151) + 1 \).
  - If a and b are integers, is \( 6a^2b \) even?
    - Yes, \( 6a^2b = 2(3a^2b) \) and \( 3a^2b \) is an integer being a product of integers: 3, a, and b.

Number theory introduction

- An integer n is **prime** if, and only if, \( n > 1 \) and for all positive integers r and s, if \( n = r \cdot s \), then either r or s equals n:
  \[ n \text{ is prime } \iff \forall \text{ positive integers } r \text{ and } s, \text{ if } n = r \cdot s \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1 \]

- An integer n is **composite** if, and only if, \( n > 1 \) and \( n = r \cdot s \) for some integers r and s with \( 1 < r < n \) and \( 1 < s < n \):
  \[ n \text{ is composite } \iff \exists \text{ positive integers } r \text{ and } s \text{ such that } n = r \cdot s \text{ and } 1 < r < n \text{ and } 1 < s < n \]

- Example: Is every integer greater than 1 either prime or composite?
  - Yes. Let n be an integer greater than 1.
    There exist at least two pairs of integers \( r = n \) and \( s = 1 \), and \( r = 1 \) and \( s = n \), s.t. \( n = rs \).
    If there exists a pair of positive integers r and s such that \( n = rs \) and neither r nor s equals either 1 or n (i.e., \( 1 < r < n \) and \( 1 < s < n \)), then n is composite. Otherwise, it’s prime.
Proving Existential Statements

- \( \exists x \subseteq D \text{ such that } Q(x) \text{ is true } \) if, and only if, \( Q(x) \text{ is true for at least one } x \text{ in } D \)

- **Constructive proofs of existence:** find an \( x \) in \( D \) that makes \( Q(x) \) true OR give a set of directions for finding such \( x \)

- **Examples:**
  - \( \exists \) an even integer \( n \) that can be written in two ways as a sum of two prime numbers
    - Proof: \( n=10=5+5=3+7 \) where 5, 3 and 7 are prime numbers
  - \( \exists \) an integer \( k \) such that \( 22r + 18s = 2k \) where \( r \) and \( s \) are integers
    - Proof: Let \( k = 11r + 9s \). \( k \) is an integer because it is a sum of products of integers. By distributivity of multiplication the equality is proved.

- **Nonconstructive proofs of existence:**
  - the evidence for the existence of a value of \( x \) is guaranteed by an axiom or theorem
  - the assumption that there is no such \( x \) leads to a contradiction

- Problem: no clue about \( x \).
Disproving Universal Statements by Counterexample

- Disprove \( \forall x \in D, \text{if } P(x) \text{ then } Q(x) \)
  - The statement is \textit{false} is equivalent to \textit{its negation is true} by giving an example
  - The negation is: \( \exists x \in D \text{ such that } P(x) \land \neg Q(x) \)
- **Disproof by Counterexample**: \( \forall x \in D, \text{if } P(x) \text{ then } Q(x) \) is false if we find a value of \( x \) in \( D \) for which the hypothesis \( P(x) \) is true and the conclusion \( Q(x) \) is false.
- \( x \) is called a \textit{counterexample}
- Example:
  - Disprove \( \forall \text{ real numbers } a \text{ and } b, \text{if } a^2 = b^2 \text{ then } a = b \)
  - \textbf{Counterexample:} Let \( a = 1 \) and \( b = -1 \).
    \[ a^2 = b^2 = 1, \text{ but } a \neq b \]

Proving Universal Statements

- Universal statement: \( \forall x \in D, \text{if } P(x) \text{ then } Q(x) \)
- \textbf{The method of exhaustion}: if \( D \) is finite or only a finite number of elements satisfy \( P(x) \), then we can try all possibilities
- Example:
  - Prove \( \forall n \in \mathbb{Z}, \text{if } n \text{ is even and } 4 \leq n \leq 7, \text{ then } n \) can be written as a sum of two prime numbers.
    - \textbf{Proof:}
      \[
      4 = 2 + 2 \quad \text{and} \\
      6 = 3 + 3 \quad \blacksquare
      \]
Proving Universal Statements

- **Method of Generalizing from the Generic Particular**
  
  suppose \( x \) is a *particular* but *arbitrarily chosen* element of the set, and show that \( x \) satisfies the property
  
  - no special assumptions about \( x \) that are not also true of all other elements of the domain

- **Method of Direct Proof:**

  1. **Statement:** \( \forall x \in D, \text{ if } P(x) \text{ then } Q(x) \)
  
  2. Let \( x \) is a particular but arbitrarily chosen element of \( D \) for which the hypothesis \( P(x) \) is true
  
  3. Show that the conclusion \( Q(x) \) is true

---

### Example

You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number.

- The result is 7 no matter what the original number is.

<table>
<thead>
<tr>
<th>Step</th>
<th>Visual Result</th>
<th>Algebraic Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pick a number.</td>
<td>( x )</td>
<td>( x )</td>
</tr>
<tr>
<td>Add 5.</td>
<td>( x + 5 )</td>
<td>( x + 5 )</td>
</tr>
<tr>
<td>Multiply by 4.</td>
<td>((x + 5) \cdot 4 = 4x + 20)</td>
<td>((x + 5) \cdot 4 = 4x + 20)</td>
</tr>
<tr>
<td>Subtract 6.</td>
<td>((4x + 20) - 6 = 4x + 14)</td>
<td>((4x + 20) - 6 = 4x + 14)</td>
</tr>
<tr>
<td>Divide by 2.</td>
<td>(\frac{4x + 14}{2} = 2x + 7)</td>
<td>(\frac{4x + 14}{2} = 2x + 7)</td>
</tr>
<tr>
<td>Subtract twice the original number.</td>
<td>((2x + 7) - 2x = 7)</td>
<td>((2x + 7) - 2x = 7)</td>
</tr>
</tbody>
</table>
Method of Direct Proof

- Example: prove that the sum of any two even integers is even
  1. Formalize: \( \forall \) integers \( m, n \), if \( m \) and \( n \) are even then \( m + n \) is even
  2. Suppose \( m \) and \( n \) are any even integers

- **Existential Instantiation:** If the existence of a certain kind of object is assumed or has been deduced then it can be given a name
  - Since \( m \) and \( n \) equal twice some integers, we can give those integers names
  - \( m = 2r \), for some integer \( r \) & \( n = 2s \), for some integer \( s \)
  - \( m + n = 2r + 2s = 2(r + s) \)
  - \( r + s \) is an integer because the sum of any two integers is an integer, so \( m + n \) is an even number
- The example can be formalized as a proved theorem

---

Example: Formal Proof

Suppose \( m \) and \( n \) are [particular but arbitrarily chosen] even integers. [We must show that \( m + n \) is even.]

By definition of even, \( m = 2r \) and \( n = 2s \) for some integers \( r \) and \( s \). Then

\[
m + n = 2r + 2s = 2(r + s)
\]

Let \( t = r + s \). Note that \( t \) is an integer because it is a sum of integers. Hence

\[
m + n = 2t
\]

where \( t \) is an integer.

It follows by definition of even that \( m + n \) is even.

[This is what we needed to show.] or [Quod Erat Demonstrandum] or Q.E.D.
Common Mistakes

1. Arguing from examples: it is true because it’s true in one particular case – **NO**
2. Using the same letter to mean two different things
3. Jumping to a conclusion – **NO, we need complete proofs!**
4. Circular reasoning: x is true because y is true since x is true
5. Confusion between what is known and what is still to be shown:
   - What is known? Premises, axioms and proved theorems.
6. Use of *any* rather than *some*
7. Misuse of *if*

Showing That an Existential Statement Is False

- The negation of an existential statement is universal:
  - To prove that an existential statement is false, we must prove that its negation (a universal statement) is true.
- Example - prove falsity of the existential statement:
  **There is a positive integer n such that n^2 + 3n + 2 is prime.**
  - The negation is:
    **For all positive integers n, n^2 + 3n + 2 is not prime.**
  Let n be any positive integer
  \[ n^2 + 3n + 2 = (n + 1)(n + 2) \]
  where \( n + 1 > 1 \) and \( n + 2 > 1 \) because \( n \geq 1 \)
  Thus \( n^2 + 3n + 2 \) is a product of two integers each greater than 1, and so it is not prime.
Rational Numbers

- A real number \( r \) is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator
  \[ r \text{ is rational} \iff \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0 \]

Examples: \( \frac{10}{3}, -\frac{5}{39}, 0.281 = \frac{281}{1000}, 7 = \frac{7}{1}, 0 = \frac{0}{1}, 0.121212 \ldots = \frac{12}{99} \)

- Every integer is a rational number: \( n = \frac{n}{1} \)

A Sum of Rationals Is Rational

- \( \forall \) real numbers \( r \) and \( s \), if \( r \) and \( s \) are rational then \( r + s \) is rational

Suppose \( r \) and \( s \) are particular but arbitrarily chosen real numbers such that \( r \) and \( s \) are rational

\[ r = \frac{a}{b} \text{ and } s = \frac{c}{d} \]

\[ r + s = \frac{ad + bc}{bd} \]

And

\[ bd \neq 0 \]

Therefore, \( r + s \) is rational.
Deriving Additional Results about Even and Odd Integers

Prove:

if a is any even integer and b is any odd integer,
then \((a^2+b^2+1)/2\) is an integer

Using the properties:

1. The sum, product, and difference of any two even integers are 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.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Suppose a is any even integer and b is any odd integer.

By property 3, \(b^2\) is odd.

By property 1, \(a^2\) is even.

By property 5, \(a^2 + b^2\) is odd.

By property 2, \(a^2 + b^2 + 1\) is even.

By definition of even, there exists an integer \(k\) such that
\[a^2 + b^2 + 1 = 2k.\]

By division with 2, \((a^2+b^2+1)/2 = k\), which is an integer.