

Discrete Mathematics

Lecture 3

Elementary Number Theory and  
Methods of Proof

Harper Langston

New York University

# Proof and Counterexample

- Discovery and proof
- Even and odd numbers
  - number  $n$  from  $\mathbb{Z}$  is called even if  $\exists k \in \mathbb{Z}, n = 2k$
  - number  $n$  from  $\mathbb{Z}$  is called odd if  $\exists k \in \mathbb{Z}, n = 2k + 1$
- Prime and composite numbers
  - number  $n$  from  $\mathbb{Z}$  is called prime if
$$\forall r, s \in \mathbb{Z}, n = r * s \rightarrow r = 1 \vee s = 1$$
  - number  $n$  from  $\mathbb{Z}$  is called composite if
$$\exists r, s \in \mathbb{Z}, n = r * s \wedge r > 1 \wedge s > 1$$

# Proving Statements

- Constructive proofs for existential statements
- Example: Show that there is a prime number that can be written as a sum of two perfect squares
- Universal statements: method of exhaustion and generalized proof
- Direct Proof:
  - Express the statement in the form:  $\forall x \in D, P(x) \rightarrow Q(x)$
  - Take an arbitrary  $x$  from  $D$  so that  $P(x)$  is true
  - Show that  $Q(x)$  is true based on previous axioms, theorems,  $P(x)$  and rules of valid reasoning

# Proof

- Show that if the sum of any two integers is even, then so is their difference
- Common mistakes in a proof
  - Arguing from example
  - Using the same symbol for different variables
  - Jumping to a conclusion
  - Begging the question

# Counterexample

- To show that the statement in the form “ $\forall x \in D, P(x) \rightarrow Q(x)$ ” is not true one needs to show that the negation, which has a form “ $\exists x \in D, P(x) \wedge \sim Q(x)$ ” is true.  $\mathbf{x}$  is called a counterexample.
- Famous conjectures:
  - Fermat big theorem: there are no non-zero integers  $x, y, z$  such that  $x^n + y^n = z^n$ , for  $n > 2$
  - Goldbach conjecture: any even integer can be represented as a sum of two prime numbers
  - Euler’s conjecture: no three perfect fourth powers add up to another perfect fourth power

# Exercises

- Any product of four consecutive integers is one less than a perfect square
- To check that an integer is a prime it is sufficient to check that  $n$  is not divisible by any prime less than or equal to  $\sqrt{n}$
- If  $p$  is a prime, is  $2^p - 1$  a prime too?
- Does  $15x^3 + 7x^2 - 8x - 27$  have an integer zero?

# Rational Numbers

- Real number  $r$  is called rational if  
 $\exists p, q \in \mathbb{Z}, r = p / q$
- All real numbers which are not rational are called irrational
- Is  $0.121212\dots$  a rational number
- Every integer is a rational number
- Sum of any two rational numbers is a rational number

# Divisibility

- Integer  $n$  is divisible by an integer  $d$ , when  
 $\exists k \in \mathbb{Z}, n = d * k$
- Notation:  $d \mid n$
- Synonymous statements:
  - $n$  is a multiple of  $d$
  - $d$  is a factor of  $n$
  - $d$  is a divisor of  $n$
  - $d$  divides  $n$

# Divisibility

- Divisibility is transitive: for all integers  $a, b, c$ , if  $a$  divides  $b$  and  $b$  divides  $c$ , then  $a$  divides  $c$
- Any integer greater than 1 is divisible by a prime number
- If  $a \mid b$  and  $b \mid a$ , does it mean  $a = b$ ?
- Any integer can be uniquely represented in the standard factored form:

$n = p_1^{e_1} * p_2^{e_2} * \dots * p_k^{e_k}$ ,  $p_1 < p_2 < \dots < p_k$ ,  $p_i$  is a prime number

# Exercises

- Prove or provide counterexample:
  - For integers  $a, b, c$ :  $(a \mid b) \rightarrow (a \mid bc)$
  - For integers  $a, b, c$ :  $(a \mid (b + c)) \rightarrow (a \mid b \wedge a \mid c)$
- If  $2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * m = 151 * 150 * 149 * 148 * 147 * 146 * 145 * 144 * 143$ , does  $151 \mid m$ ?
- Show that an integer is divisible by 9 iff the sum of its digits is divisible by 9. Prove the same for divisibility by 3.
- Show that an integer is divisible by 11 iff the alternate sum of its digits is divisible by 11

# Quotient and Remainder

- Given any integer  $n$  and positive integer  $d$ , there exist unique integers  $q$  and  $r$ , such that  $n = d * q + r$  and  $0 \leq r < d$
- Operations: `div` – quotient, `mod` – remainder
- Parity of an integer refers to the property of an integer to be even or odd
- Any two consecutive integers have opposite parity
- The square of an odd integer has remainder 1 when divided by 8 (read in book)

# Exercises

- Show that a product of any four consecutive integers is divisible by 8
- Show that the sum of any four consecutive integers is never divisible by 4
- Show that any prime number greater than 3 has remainder 1 or 5 when divided by 6

# Floor and Ceiling

- For any real number  $x$ , the floor of  $x$ , written  $\lfloor x \rfloor$ , is the unique integer  $n$  such that  $n \leq x < n + 1$ . It is the max of all ints  $\leq x$ .
- For any real number  $x$ , the ceiling of  $x$ , written  $\lceil x \rceil$ , is the unique integer  $n$  such that  $n - 1 < x \leq n$ . What is  $n$ ?
- If  $x$  is an integer, what are  $\lfloor x \rfloor$  and  $\lfloor x + 1/2 \rfloor$ ?
- Is  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ ?
- For all real numbers  $x$  and all integers  $m$ ,  $\lfloor x + m \rfloor = \lfloor x \rfloor + m$
- For any integer  $n$ ,  $\lfloor n/2 \rfloor$  is  $n/2$  for even  $n$  and  $(n-1)/2$  for odd  $n$
- For positive integers  $n$  and  $d$ ,  $n = d * q + r$ , where  $d = \lfloor n / d \rfloor$  and  $r = n - d * \lfloor n / d \rfloor$  with  $0 \leq r < d$

# Exercises

- Is it true that for all real numbers  $x$  and  $y$ :
  - $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$
  - $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$
  - $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$
  - $\lceil x + 1 \rceil = \lceil x \rceil + 1$
- Show that for all real  $x$ ,  $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor x/4 \rfloor$

# Contradiction

- Proof by contradiction
  - Suppose the statement to be proved is false
  - Show that this supposition leads logically to a contradiction
  - Conclude that the statement to be proved is true
- The sum of any rational number and any irrational number is irrational

# Contraposition

- Proof by contraposition
  - Prepare the statement in the form:  $\forall x \in D, P(x) \rightarrow Q(x)$
  - Rewrite this statement in the form:  $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$
  - Prove the contrapositive by a direct proof
- For any integer, if  $n^2$  is even then  $n$  is even
- Close relationship between proofs by contradiction and contraposition

# Exercise

- Show that for integers  $n$ , if  $n^2$  is odd then  $n$  is odd
- Show that for all integers  $n$  and all prime numbers  $p$ , if  $n^2$  is divisible by  $p$ , then  $n$  is divisible by  $p$
- For all integers  $m$  and  $n$ , if  $m+n$  is even then  $m$  and  $n$  are both even or  $m$  and  $n$  are both odd
- The product of any non-zero rational number and any irrational number is irrational
- If  $a$ ,  $b$ , and  $c$  are integers and  $a^2+b^2=c^2$ , must at least one of  $a$  and  $b$  be even?
- Can you find two irrational numbers so that one raised to the power of another would produce a rational number?

# Classic Number Theory Results

- Square root of 2 is irrational
- For any integer  $a$  and any integer  $k > 1$ ,  
if  $k \mid a$ , then  $k$  does not divide  $(a + 1)$
- The set of prime numbers is infinite

# Exercises

- Show that
  - a square of 3 is irrational
  - for any integer  $a$ , 4 does not divide  $(a^2 - 2)$
  - if  $n$  is not a perfect square then its square is irrational
  - $\sqrt{2} + \sqrt{3}$  is irrational
  - $\log_2(3)$  is irrational
  - every integer greater than 11 is a sum of two composite numbers
  - if  $p_1, p_2, \dots, p_n$  are distinct prime numbers with  $p_1 = 2$ , then  $p_1 p_2 \dots p_n + 1$  has remainder 3 when divided by 4
  - for all integers  $n$ , if  $n > 2$ , then there exists prime number  $p$ , such that  $n < p < n!$

# Algorithms

- Algorithm is step-by-step method for performing some action
- Cost of statements execution
  - Simple statements
  - Conditional statements
  - Iterative statements

# Division Algorithm

- Input: integers **a** and **d**
- Output: quotient **q** and remainder **r**
- Body:
  - $r = a; q = 0;$
  - while ( $r \geq d$ )
    - $r = r - d;$
    - $q = q + 1;$
  - end while

# Greatest Common Divisor

- The greatest common divisor of two integers  $a$  and  $b$  is another integer  $d$  with the following two properties:
  - $d \mid a$  and  $d \mid b$
  - if  $c \mid a$  and  $c \mid b$ , then  $c \leq d$
- Lemma 1:  $\gcd(r, 0) = r$
- Lemma 2: if  $a = b * q + r$ , then  $\gcd(a, b) = \gcd(b, r)$

# Euclidean Algorithm

- Input: integers **a** and **b**
- Output: greatest common divisor **gcd**
- Body:
  - $r = b;$
  - while ( $b > 0$ )
    - $r = a \bmod b;$
    - $a = b;$
    - $b = r;$
  - end while
  - $\text{gcd} = a;$

# Exercise

- Least common multiple: lcm
- Prove that for all positive integers  $a$  and  $b$ ,  
 $\gcd(a, b) = \text{lcm}(a, b)$  iff  $a = b$