CS 173: Discrete Structures

Eric Shaffer
Office Hour: Wed. 12-1, 2215 SC
shaffer1@illinois.edu

Agenda

We will discuss basic number theory

- Section 3.4
  - "division algorithm"
  - modular arithmetic
- Section 3.5
  - prime numbers
  - gcd, lcm

What proof techniques have we seen?

Direct
Contradiction
Contraposition

Lightning Round

- 4 | 24 T
- 0 | 24 F
- 24 | 0 T

- What is the definition of divisor?

For $a, b \in \mathbb{Z}$ we say $a \mid b$ if $\exists k \in \mathbb{Z}$ s.t. $b = ak$

Perfect squares and even numbers

- Just for practice, let's prove:

For any integers a and k, if $a^2 = 2k$ then a is even

P Q

Contrapositive:

If a is odd, then a^2 is odd

$a = 2j+1$ since a is odd, $j \in \mathbb{Z}$

$a^2 = (2j+1)^2 = 4j^2 + 4j + 1$

$= 2(2j^2 + 2j) + 1$

so, by def., a^2 is odd

Perfect squares and even numbers

For any integers a and k, if $a^2 = 2k$ then a is even $\equiv \neg(a^2 = 2k) \vee a \text{ is even}$

Using contradiction

Contradiction

we assume $a^2 = 2k$ $\wedge$ a is odd

a^2 is even

If a is odd then $a = 2j + 1$ for some $j \in \mathbb{Z}$

So $a^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1$

a^2 is odd contradicts

Direct Proof

~~Proof by contradiction~~

- Prove: Every list of numbers contains a number as large as the average.

at least

Given a list $a_1, a_2, \ldots, a_n$ for $n \in \mathbb{N}$

$\exists\, a_k$ such that $a_k \geq \frac{\sum_{i=1}^{n} a_i}{n}$

Let a_k be largest in list

$\underbrace{a_k + a_k + \ldots + a_k}_{n a_k} \geq a_1 + a_2 + \ldots + a_n$

so $n a_k \geq \sum_{i=1}^{n} a_i \rightarrow a_k \geq \frac{\sum_{i=1}^{n} a_i}{n}$

Proof by contradiction

- Prove: Every list of numbers contains a number as large as the average.

at least

Given a list $a_1, a_2, \ldots, a_n$ for $n \in \mathbb{N}$

Assume negation of the claim:

$\forall a_i,\ a_i < \frac{1}{n}\left(\sum_{i=1}^{n} a_i\right)$

Let a_k be largest in list

$$\underbrace{a_k + a_k + \ldots + a_k}_{n a_k} \geq a_1 + a_2 + \ldots + a_n$$

so $n a_k \geq \sum_{i=1}^{n} a_i$ → contradict

$$a_k \geq \frac{\sum_{i=1}^{n} a_i}{n}$$

Proof by contraposition

- If (3n+1) is even then n is odd

if n is even then (3n+1) is odd.

So $n = 2k$ for some $k \in \mathbb{Z}$

If follows $3n+1 = 3(2k)+1$

$= \underbrace{2(3k)+1}_{\text{odd}}$

by def. 3n+1 is odd

The division "algorithm"

Let a be an integer and d a positive integer. Then there are unique integers q and r such that $a = dq + r$ with $0 \leq r < d$

As stated, it's not really an algorithm (why not?)

Terminology:

- d is the divisor
- a is the dividend
- q is the quotient
- r is the remainder

mod function

mod is a binary function

Let $a = dq + r$, then we say a **mod** $d = r$

Note:

- d is a positive integer (by definition)
- r is a positive integer (by definition)
- a is not necessarily positive

Q: Compute

113 **mod** 24 = 17

-29 **mod** 7 = 6

mod function

-29 **mod** 7

We have -29 = 7(-5) + 6

This is not always correctly implemented in programming languages!

-10 **mod** 3 = 2, but in Java –10%3 = -1

Challenge:

What languages implement this correctly?

Which implement it incorrectly?

python

Modular Arithmetic

$3 \equiv 9 \bmod 2$

The word "mod" is used in two ways:

- the **mod** function
  - Inputs a number *a* and a base *m*
  - Outputs *a* **mod** *m* a number between 0 and *m* -1 inclusive
  - This is the remainder of $a \div m$

$10 \equiv 100 \bmod 2$

- the (mod) congruence predicate
  - Relates two numbers *a*, *b* to each other relative some base *m*

$a \equiv b \pmod{m}$

means that *a* and *b* have the same remainder when dividing by *m*

(mod) congruence

DEF: Let a,b be integers and m be a positive integer. We say that a is congruent to b modulo m (denoted by $a \equiv b \pmod{m}$) iff $m \mid (a - b)$.

Equivalently: $a \bmod m = b \bmod m$

Q: Which of the following are true?

1. $3 \equiv 3 \pmod{17}$ T
2. $3 \equiv -3 \pmod{17}$ F
3. $172 \equiv 177 \pmod{5}$ T
4. $-13 \equiv 13 \pmod{26}$ T

$3 \bmod 17 = 3$

$-3 \bmod 17 = 14$

$-3 = 17(-1) + 14$

$172 \bmod 5 = 2$

(mod) congruence

iff

$p \leftrightarrow q$

$p \rightarrow q$

$q \rightarrow p$

THM: Let *m* be a positive integer

Integers *a* and *b* are congrent modulo m if an only if
there is an integer *k* such that $a = b+km$

Proof: p

If *a* and *b* are congruent mod *m* then

1. $m|(a-b)$
2. $(a-b) = km$
3. $a = b+ km$

.....and we need to prove the converse as well... $q \rightarrow p$

if $a = b + km$ then $a \equiv b \bmod m$

$(a-b) = km$

which means $m|(a-b)$

by def $\equiv \bmod m$ $a \equiv b \bmod m$

(mod) congruence identities

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$
Then:

$a+c \equiv b+d \pmod{m}$

(mod) congruence identities

THM:

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

$ac \equiv bd \pmod{m}$

Greatest Common Divisor

- Definition: Let a and b be integers (not both 0)
  - Let d be the largest integer with $d|a$ and $d|b$
  - d is called the **greatest common divisor** of a and b
  - written as **gcd(a,b)**

- Integers a and b are **relatively prime** if gcd(a,b)=1

Greatest Common Divisor

- Define gcd in terms of the prime factorizations of a,b

Least Common Multiple

- Definition: Let a and b be positive integers
  - Let m be the smallest integer with $a|m$ and $b|m$
  - m is called the **least common multiple** of a and b
  - written as **lcm(a,b)**

Least Common Multiple

- Define lcm in terms of the prime factorizations of a,b

- What is lcm(a,b)gcd(a,b)?

An infinite number of primes…

- Consider the formula from the proof: $k = (p_1 p_2 \ldots p_m + 1)$
- Note that k is prime ONLY IF p_m is the largest prime
  - Have we proved k will be a prime in the "real world"?

  - How can we prove whether or not k will be prime?
    - Disprove using a counter-example
    - Consider (2•3•7•11)+1= 30031

An infinite number of primes…

Some interesting facts….

- No known formula generates all primes
- No known formula generates only primes
- Some formulas generate only 1's and primes:
  - For example:

    For $n \geq 2$, set $a(n) = a(n-1) + \gcd(n, a(n-1))$

    In a paper by Rowland, Aug. 2008

Announcements

- HW 2 posted on website (due Friday the 13th)
- Quiz Wed. Feb. 11th, end of class
  - 15 minutes
  - Covers through the end of this week
  - "Skills list" on the course website
    - http://www.cs.uiuc.edu/class/sp09/cs173/Exams/