CS 173: Discrete Structures

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

Announcements

- Quiz Wed. Feb. 11th, end of class
  - Covers through the end of this week (Feb. 6th)
  - Specific topics will be posted on web (by Fri.)
  - 15 minutes at the end of class
  - Short answer (possibly some TF)
  - Old Quiz:
    http://www.cs.uiuc.edu/class/fa08/cs173/Exams/quiz1-answers.pdf

Before we get started…

- Super-secret tip for doing well in the class:
  - Read the book
- About the lecture notes…
  - I'm using powerpoint…you probably figured that out
  - You should consider taking your own notes
    - Especially if you can't read my writing
    - Reviewing will be easier
- Does anyone know what "discrete" means?

Discrete Mathematics

- "**Discrete mathematics** is the study of mathematical structures that are fundamentally discrete in the sense that its objects can assume only distinct, separate values, rather than a values on a continuum"
  - Thank you Wikipedia…
  - It's the difference between **N** and **R**
- Discrete mathematics includes the following topics:
  - Logic - a study of reasoning
  - Set theory - a study of collections of elements
  - Number theory
  - Combinatorics
  - Graph theory
  - Algorithmics
  - Partially ordered sets
  - Proofs
  - Relations

Agenda

- Proof techniques (section 1.6)
  - Proof by contraposition
  - Proof by contradiction

- To practice proof techniques, we need things to prove
  - We will discuss basic number theory
    - Sections 3.4
    - Section 3.5

Number Theory

- The branch of mathematics that deals with the properties of numbers, the integers in particular

- Applications of Number Theory:
  - Cryptology (science of secure communication)
    - CS 461 Computer Security I
  - Data Structures (hash tables)
    - CS 225
  - Random number generation
  - Music
    - The distribution of normal modes in rooms

Divisors

DEF: Let a, b and c be integers such that

$$a = bc$$

Then b and c are said to divide (or are factors) of a

- a is said to be a multiple of b (as well as of c).
- the pipe symbol "|" denotes "divides":

  $b \mid a \quad \wedge \quad c \mid a$
- NOTE: Don't confuse the order:

  $b \mid a$ means b divides a (same order as the sentence).

Divisors

Which of the following are true?

- 77 | 7
- 7 | 77
- 24 | 24
- 0 | 24
- 24 | 0

Divisors

- $77 \mid 7$: false
- $7 \mid 77$: true because $77 = 7 \cdot 11$
- $24 \mid 24$: true because $24 = 24 \cdot 1$
- $0 \mid 24$: false, only 0 is divisible by 0
- $24 \mid 0$: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Number of Multiples of d up to given n

Q: How many positive multiples of 13 are less than 100?

$\frac{100}{13} = 7\frac{9}{13}$

Q: Generalize this, state formula for d and n

$\left\lfloor \frac{n}{d} \right\rfloor$

The Divisor Theorem

THM: Let a, b, and c be integers. Then:

1. $a|b \wedge a|c \rightarrow a|(b + c)$
2. $a|b \rightarrow a|bc$
3. 3. $a|b \wedge b|c \rightarrow a|c$

Can you prove this ? Let $a|b \wedge a|c$

Then $b = ak$ and $c = aj$

It follows $b + c = ak + aj = a(k+j)$

we know $a|a(k+j)$

so $a|(b+c)$

Divisor Theorem

In a direct proof, statements are proved by starting from the definitions and manipulating to get the desired results.

Proof of $a|b \rightarrow a|bc$

Suppose $a|b$

By definition, there is a number m such that $b = am$

Multiply both sides by c to get $bc = amc$

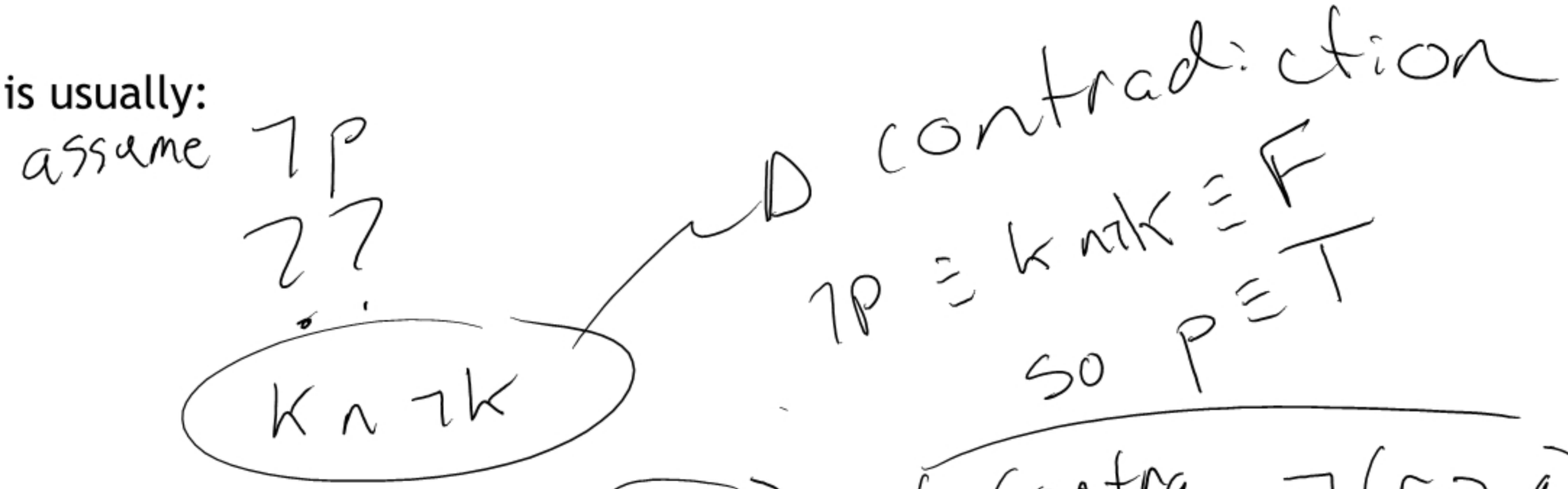
So, $bc = a(mc)$

- Consequently, bc has been expressed as a times the integer mc so by definition of "|", $a|bc$

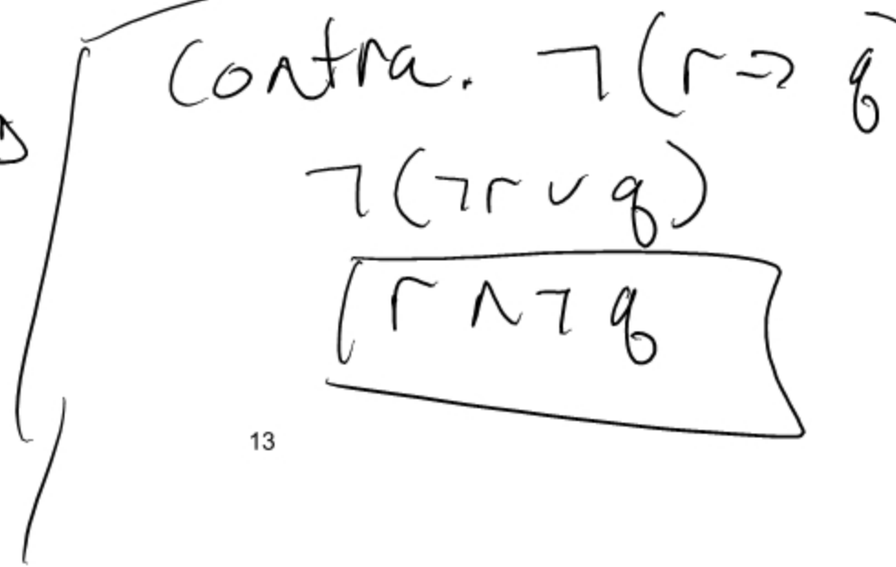
Proof by Contradiction

To prove a proposition **p**, assume **¬p** and show a contradiction

- Basic form is usually:



- Suppose the proposition **p** is of the form **r → q**
  - recall that **r → q ≡ q ∨ ¬r ≡ ¬(¬q ∧ r)**.
  - So assuming the negation is to assume **¬q ∧ r**



For direct
assume r ≡ T

Prove that √2 is irrational

- A ***rational number*** can expressed as a/b
  - where a and b are integers
  - and a and b share no common factors
- Can all numbers be expressed this way?
- Hippasus (500 BC) was a student of Pythagoras
  - proved √2 cannot be expressed as a ratio
  - …which posed serious problems for Greek mathematics

Prove that √2 is irrational

Assume $\sqrt{2} = \frac{a}{b}$ w/ a ∧ b having no common factors

$2 = \frac{a^2}{b^2}$

$2b^2 = a^2$ so $a = 2k$

$2b^2 = (2k)^2 = 4k^2$

$b^2 = 2k^2$ so $b = 2j$

$2|a \wedge 2|b$ contradicts

So $\sqrt{2}$ is irrational

Prove that $\sqrt{2}$ is irrational

Assume the negation:

$\sqrt{2} = a/b$, with a and b sharing no common factors

$2 = a^2/b^2$

$2b^2 = a^2$

a^2 is even, and so a is even ($a = 2k$ for some k)

$b^2 = 2k^2$

$2b^2 = (2k)^2 = 4k^2$

b^2 is even, and so b is even ($b = 2k$ for some k)

Proof by Contraposition

Recall that $p \rightarrow q \equiv \neg q \rightarrow \neg p$ (the contrapositive)

So, we can prove the implication $p \rightarrow q$
by first assuming $\neg q$, and showing that $\neg p$ follows

Example: Prove that for integers a and b,
$(a + b \geq 15) \rightarrow (a \geq 8) \vee (b \geq 8)$

p q

1. (Assume $\neg q$) Suppose $(a < 8) \wedge (b < 8)$
2. (Show $\neg p$) Then $(a \leq 7) \wedge (b \leq 7)$,
3. So $(a + b) \leq 14$,
4. and it follows that $(a + b) < 15$. $\neg p$

Proof by Contraposition

"if x is a perfect square, and x is even, then x is divisible by 4."

Formally: $(p \wedge q) \rightarrow r$

Contrapositive: $\neg r \rightarrow \neg(p \wedge q)$

If x is not divisible by 4 equivalent to saying:

$x = 4k + 1$, or $x = 4k + 2$, or $x = 4k + 3$

Now structure looks like $(u1 \vee u2 \vee u3) \rightarrow (\neg p \vee \neg q)$

- Case 1 (&3): x = 4k + 1, odd, implies ¬q
- Case 2: x = 4k + 2, even, so must not be a perfect square.

Proof by Contraposition

- Case 2: x = 4k + 2, even, so must not be a perfect square.
  Proof:
  1. $x = 4k + 2 = 2(2k + 1)$
  2. x is the product of 2 and an odd number.
  3. so, x is not a perfect square.

$\neg P$

e.g.
$a = 2j$
$a^2 = 2^2 j$

Prime Numbers

DEF: A number n ≥ 2 ***prime*** if it is only divisible by 1 and itself

A number $n \geq 2$ which isn't prime is called **composite**

Q: Which of the following are prime?

0,1,2,3,4,5,6,7,8,9,10

Fundamental Theorem of Arithmetic

THM: Any number $n \geq 2$ is expressible as as a unique product of 1 or more prime numbers.

- Almost proved by Euclid
- First full and correct proof by Carl Friedrich Gauss

We'll need induction and some more number theory tools to prove this.

Q: Express each of the following number as a product of primes: 22, 100, 12, 17

$22 = 2 \cdot 11$

$100 = 2^2 \cdot 5^2$

$12 = 2^2 \cdot 3$

$17 = 17$

There are infinitely many primes...Euclid (300 BC)

- Prove it by contradiction

Assume finite # of primes

Let p_n be largest prime

Let $m = p_1(p_2 \cdots p_n) + 1$

where p_i is a prime

$m > p_n$

For any p_i, $p_i \nmid m$

It follows m is prime

There are infinitely many primes…Euclid (300 BC)