MATH 22

Lecture A: 9/2/2003

THEMES

This is a wretched beginning, indeed!
—Jane Austen, *Pride and Prejudice*, ch. 59

La distance n'y fait rien; il n'y
a que le premier pas qui coûte.
—Mme du Deffand

(sorry; no Russian font for
the original of the Pushkin;
hope you copied it down in class!)

Today: Introduction; course themes; proofs with examples; prime numbers, primality testing and the Sieve of Eratosthenes (4.3)

The distance is nothing; it is only the first step that is difficult.

—Mme du Deffand

He had the talent of saluting
felicitously every theme, . . .
or, with an epigram-surprise,
of kindling smiles in ladies' eyes.

— Pushkin, *Eugene Onegin,* I:5

Administrivia I: Course

- **Description**

  Sets, relations and functions, logic and methods of proof, combinatorics, graphs and digraphs. Partially true.

- **Home Page**

  http://www.tufts.edu/~melder01/22.html

- **Prerequisites**

  Mathematics 11 or Computer Science 11 or consent.

- **Textbooks**

  Ralph P. Grimaldi, *Discrete and Combinatorial Mathematics,* **fifth** edition, Addison-Wesley 2003.

  Lewis, et. al., *Data Structures and Their Algorithms,* Harper-Collins 1991.

- **Syllabus Handout**

- **Problem sets, exams, grading**

  (All on the course homepage!)

Administrivia II: Section

- **Instructor**

  Larry Denenberg, larry@denenberg.com
  Office hours Thursday after class or by appointment, BP 214
  Phone 617-995-1234 during the day
  http://larry.denenberg.com/

- **Location**

  Here.

- **Lectures**

  Presentation of the same material, sometimes from a slightly different viewpoint to enhance understanding (but your formal responsibility is to the syllabus and the textbook!)

  Questions answered; obscure points cleared up; related topics explored; entertainment offered; dragons slain

- **Lecture notes**

  Posted on the web (location TBD; possibly the course site) but not handed out physically due to budgetary constraints

  Use them in place of notetaking, or to take notes upon, or after class for review—your choice. (Choose based on personal learning style; it's worth finding your best mode!)

Theme I: Proofs

What is a (mathematical) proof? Theorems vs. lemmata, corollaries, and conjectures. Good & bad proofs. Kinds of proof. Logic. Famous proofs.

Goals:

- Read and appreciate proofs
- Write correct and literate proofs

Theme II: Algorithms

What is an algorithm? What properties must an algorithm have? How do we measure the "goodness" of an algorithm? Some formalizations (maybe).

Goals:

- Know how algorithms differ from proofs
- Learn a little about algorithm analysis

Theme III: Notation

Thirty percent of mathematical maturity is fearlessness in the face of symbols: the ability to read and understand notation, to introduce clear and useful notation when appropriate (and not otherwise!), and a general facility of expression in the terse—but crisp and exact—language that mathematicians use to communicate ideas. Mathematics, like English, relies on a common understanding of definitions and meanings. But in mathematics definitions and meanings are much more often attached to symbols, not to words, although words are used as well. Furthermore, the definitions are much more precise and unambiguous, and are not nearly as susceptible to modification through usage. You will never see a mathematical discussion without the use of notation!

What is a proof?

According to the dictionary, . . . [never do this! never!]

A proof of a fact is *any argument that convinces you of that fact*.

But: What is an argument? What does "convinces" mean? Who is "you" in this definition? What does "obvious" mean?

Mathematical proof is a (partially successful) way to standardize answers to these problems: A mathematical proof is a chain of reasoning leading from assumptions to a conclusion, where each step follows from accepted logical principles and uses no facts or information that have not previously been proved.

Proof vs. definition. A definition is not a proof!

What makes a good proof, an elegant proof, an artistic proof? Proof as artistic expression. (Erdös' book)

Logic: A formalization of the notion of proof.

Kinds of proof: Construction, contradiction, mathematical induction, infinite descent, diagonalization, . . .

Computer proofs

Our First Theorem

Theorem I: For all positive integers n,

$$1 + 2 + 3 + \ldots + n = n(n+1)/2$$

We can write this more compactly as

$$\sum_{i=1}^{n} i = n(n+1)/2$$

Examples:

- $n = 3$: $1+2+3 = 6 = (3)(3+1)/2$
- $n = 6$: $1+2+3+4+5+6 = 21 = (6)(7)/2$
- $n = 1$: $1 = (1)(2)/2$

How can we *prove* this for **all** n?

Nonmathematical Proofs

Proof B1: It's true because it says so in the Bible. (Or the Qur'an, or my father said so, or Larry says so.) [Proof by authority]

Proof B2: It's true because I tried it for many values and never found it wrong. [Proof by inductive reasoning]

Proof B3: It's true because Dan Quayle says it's false. (Or Larry says it's false.) [Proof by ad hominem argumentation]

Proof B4: It's true because if you don't believe it I'll break your neck (or give you an F in Math 22). [Proof by intimidation]

Proof B5: It's true since $2n = 1+(n-1)+n$ therefore $n(n+1) = n^2 + n$ and so the conclusion follows. [Non sequitur]

All of these are *nonmathematical* proofs, often used in the real world.

Proof by Mathematical Induction

(not to be confused with inductive reasoning; cf vos Savant)

Suppose we have a statement S about a number n. (We write S_n for such a statement.) Suppose that we can prove two things:

- The statement is true for 1, that is, S_1 is true.
- Assuming that the statement is true for an unspecified number n, we can prove the statement true for $n+1$, that is, S_n *implies* S_{n+1}.

We can conclude that S_n is true for all $n \geq 1$.

This is the *Principle of Mathematical Induction*, which in this class we just assume to be true (though it does need to be proved!).

But it's at least intuitive: we know S_1, and from S_1 we know S_2, and from S_2 we know S_3, and so forth, which means S_n is true for all n.

Our First (Real) Proof

We are going to prove Theorem 1 by mathematical induction. The statement about n, S_n, is that $1 + 2 + 3 + \ldots + n = n(n+1)/2$.

By the Principle, there are two things to show:

- S_1 is true, i.e., $1 = (1)(2)/2$, clearly true.
- S_n implies S_{n+1}. That is, assuming S_n is true, we need to prove S_{n+1}, i.e., we must prove that

$$1+2+3+ \ldots + n + (n+1) = (n+1)(n+2)/2$$

Think of the LHS as $(1+2+3+\ldots+n) + (n+1)$. Since we know S_n is true, we can rewrite it as

$$(n(n+1)/2) + (n+1)$$

and a little algebra turns this into $(n+1)(n+2)/2$ which is what S_{n+1} says it should be. All done.

[Much more on mathematical induction later in the course.]

A Prettier Proof

The sum we're looking for, call it X, is:

$$1 + 2 + 3 + \ldots + (n-1) + n$$

But X is also equal to:

$$n + (n-1) + (n-2) + \ldots + 2 + 1$$

Adding these, it follows that 2X equals:

$$(n+1)+(n+1)+(n+1)+\ldots+(n+1)+(n+1)$$

This sum consists of n copies of (n+1), so we have

$$2X = n(n+1)$$

or

$$X = n(n+1)/2$$

which is the result we're looking for!

(This last line is often written QED, that is, "quod erat demonstrandum", or just .)

Is this a better proof? (Let's look at a picture!) Good proofs help to promote understanding, they're not just globs of rigor or formalism!

New Topic: Primes

Let $n>1$ be an integer. We say that n is *composite* if $n = ab$ for two integers a and b (not necessarily distinct) each of which is > 1.

If n is not composite, then n is called *prime*.

(1 itself is neither prime nor composite—it's called a *unit*. The text has a different but equivalent definition using *divisors*: $a|b$ means that there is no remainder when b is divided by a, and n is prime if it has exactly two positive divisors, itself and 1.)

Examples:

- 6 is composite, since 6 = (2)(3).
- 24 is composite, since 24 = (6)(4).
- 9 is composite, since 9 = (3)(3).
- 3, 7, 11, 37, 91, and 5882352941 are prime [careful!].

Two questions naturally arise:

- How many primes are there?
- Given a number, how do we tell whether it's prime? (How did I know about 5882352941?)

How Many Primes?

It has been known since the time of Euclid, 2300 years ago, that there are an infinite number of primes.

We prove this fact *constructively* as follows: Given any finite set $\{p_1, p_2, \ldots, p_n\}$ of primes we will construct a new prime p that's not in the set! Of course we can then use the same construction to make new primes endlessly.

Lemma (eh?): If n is composite, then there is some prime p that divides n (proved on page 222 using concepts from earlier sections).

Proof (of main theorem): Given the set of primes as above, let $a = 1 + p_1p_2p_3\ldots p_n$. Since $a > 1$ there are two possibilities:

- a is prime. But a is clearly not one of the p_i (it's too big) so a is a new prime.

(continued...)

• a is composite. Then by the Lemma there is a prime p that divides a. But clearly none of the p_i in our set divide a, since dividing a by any of the p_i will leave remainder 1! So p is not equal to any of the p_i and thus is a new prime.

In either case, we've constructed a new prime as promised and we're done. QED

Comment: The text recasts essentially the same proof as proof by *contradiction*. That is:

Suppose we assume that a statement S is false, and using this assumption we can prove a contradiction (that is, a patently false statement, like 1=2). Then statement S is true!

The proof in the text starts by assuming there are a finite number of primes $p_1, p_2, \ldots, p_k$, and concluding that one of these primes must divide 1, an absurdity. It follows that there cannot be a finite number of primes.

Algorithms

Now for the second question: How do we test a given number to see whether it's prime?

What we're looking for is not the same thing as a proof! We can prove that a *specific* number (e.g. 91) is or is not prime, but here we want a "method" that works on an *arbitrary* number, not given in advance.

Such a method is called an *algorithm*. An algorithm is a computational procedure used for solving a problem; it takes some input and produces some output. To be an algorithm, a computational procedure must be:

1. *Effective*, that is, able to be rendered as a computer program.
2. *Correct*. An algorithm must never give the wrong answer.
3. *Terminating*. An algorithm must eventually stop with an answer.

An interaction between algorithms and proof is that we usually must *prove* these properties of our algorithms!

Algorithms for primality testing

Algorithm 1: Given n, check to see if it is divisible by 2, 3, 4, 5, 6, 7, . . . , n-1. If the answer is always NO, n is prime.

Are the effectiveness, correctness, and termination of this algorithm obvious? What are the inputs and outputs?

Algorithm 2: Given n, check to see if it is divisible by 2, 3, 4, 5, 6, 7, . . . , floor($\sqrt{n}$). If the answer is always NO, n is prime.

Just as obviously effective and terminating, but maybe not so obviously correct. Why does it work?

(Notation: floor(x) is the greatest integer less than x, i.e., x rounded down to the next smallest integer.)

Although both of these are algorithms, Algorithm 2 is better than Algorithm 1 because it's (obviously) faster. How much faster? How do you measure the speed of an algorithm anyway? In what other ways might one algorithm be better than another? We'll take up these questions later in the course.

Another primality algorithm

Algorithm 3: Given n, check to see if it is divisible by 2, 3, 5, 7, 11, 13, . . . , floor($\sqrt{n}$), that is, by all primes up to (the floor of) its square root. If the answer is always NO, n is prime.

Again, we must take a moment to convince ourselves of the correctness of this algorithm. You may also raise the question of effectiveness, since somehow we need to have at hand a list of the primes, and we need a primality tester to generate them!

The Sieve of Eratosthenes

(air uh TAHZ the knees)

Here is an algorithm, 2200 years old, for finding all the primes from 2 up to any number N (where N is specified in advance):

Step 1: Write down all the integers from 2 up to N. All numbers start "unmarked".

Step 2: Let p be the smallest unmarked number on the list. Mark it as prime.

Step 3: Starting with $2p$, mark every p^{th} number on the list as composite.

Step 4: If there are any unmarked numbers on the list, go back to Step 2. Otherwise, stop.

(As usual, we must satisfy ourselves of the effectiveness, correctness, and termination of this algorithm.)

(Pretty sieve picture drawn on blackboard.)

Twin Primes

Suppose two numbers p and $p+2$ are both prime. Such numbers are called *twin primes*.

Examples: 11 & 13, 41 & 43, 107 & 109.

Question: How many twin primes are there? The answer is that nobody knows. It seems likely that there are an infinite number, but nobody has proved it either way. That is, we *conjecture* that there are an infinite number of twin primes. (Why is this a hard problem?)

Three numbers p, $p+2$, and $p+4$ that are all prime are called *triplet primes* (a term I just invented). For example, 3, 5, and 7 are triplet primes. It isn't too hard to prove that there **aren't** an infinite number of triplet primes; in fact, 3, 5, and 7 are the **only** triplet primes! Can you prove this? Hint: Why can't two numbers p and $p+1$ both be prime, except 2 and 3? As another hint, you might think about what the Sieve does to any three numbers p, $p+2$, $p+4$.