Math 55

class notes

6/25/2007 Monday

What is discrete math? Other words that describe "discrete" are: separate, countable, distinguishable, distinct, and unconnected.

Here's what the book says (page xx):

> **W**hat is discrete mathematics? Discrete mathematics is the part of mathematics devoted to the study of discrete objects. (Here *discrete* means consisting of distinct or unconnected elements.) The kinds of problems solved using discrete mathematics include:
>
> - How many ways are there to choose a valid password on a computer system?
> - What is the probability of winning a lottery?
> - Is there a link between two computers in a network?
> - How can I identify spam e-mail messages?
> - How can I encrypt a message so that no unintended recipient can read it?
> - What is the shortest path between two cities using a transportation system?
> - How can a list of integers be sorted so that the integers are in increasing order?
> - How many steps are required to do such a sorting?
> - How can it be proved that a sorting algorithm correctly sorts a list?
> - How can a circuit that adds two integers be designed?
> - How many valid Internet addresses are there?
>
> You will learn the discrete structures and techniques needed to solve problems such as these.
>
> More generally, discrete mathematics is used whenever objects are counted, when relationships between finite (or countable) sets are studied, and when processes involving a finite number of steps are analyzed. A key reason for the growth in the importance of discrete mathematics is that information is stored and manipulated by computing machines in a discrete fashion.

Some of the main types of things we'll be doing are:

1. Learning how to construct proofs.
2. Learning how to count things.
3. Learning how to think algorithmically

We'll also be spending a good deal of time on number theory (the study of divisibility and remainders) and graph theory (the study of dots with lines between them).

Let's look at some examples of problems we will study this term:

— Example 1: Birthdays: (some counting problems: ch 3, 5, 6)

— Q: How many ways can I guess all 23 students' birthdays?

A: $365 \cdot 365 \cdot \cdots \cdot 365 = 365^{23}$

— Q: What if I don't allow repeats?

A: $365 \cdot 364 \cdot \cdots \cdot 343 = 365! / 23!$ [← we'll learn what this means] (ch 5)

— Q: How many peope do we need to be present to guarantee a repeated birthday?

A: 366: If there's 365 people we can give each one a different birthday. But when the 366^{th} person comes in, there's no unused dates left to give them.

— Q: What is the probability that in a room of 23 people, some two people have the same birthday?

A: We will find out later! [The answer may surprise you] (ch. 6).

— Q: Can you come up with a method or algorithm for finding repeated birthdays in a group of people?

A: Try it! [We will study the efficiency of different such algorithms] (ch 3)

— Example 2: Numbers: (set theory and number theory: ch 2, 3).

(a) We know that an integer n is divisible by 3 if the sum of its digits is divisible by 3. But why?

Let's take $n = 4203$ and write it as $n = 4 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^0$. Next observe that any power of ten will have a remainder of 1 when divided by 3. So if we just look at the remainder of n when we divide by 3, we get remainder $= 4 \cdot 1 + 2 \cdot 1 + 3 \cdot 1 = 4 + 2 + 3 = 9$ = the sum of the digits of n. Then the remainder of 9 divided by 3 is zero, which means 9 is divisible by 3, and so is 4203.

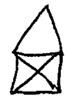
[We will learn why this makes sense and other similar tricks] (ch 3)

(b) The following boxes are ordered by the number of things in them:

$\underset{0}{\boxed{}} < \underset{1}{\boxed{9}} < \underset{\text{some finite number}}{\boxed{\text{all the atoms in the universe}}} < \underset{\infty}{\boxed{1, 2, 3, \cdots}} = \underset{\infty}{\boxed{2, 4, 6, \ldots}} = \underset{\infty}{\boxed{\text{All fractions}}} < \underset{\infty}{\boxed{\text{All numbers between 0 and 1}}}$

[We will learn how to compare different sizes of infinity] (ch 2)

— Example 3: Houses (Graph theory: ch 9)

Can you draw this:  without lifting your pencil or retracing any lines?

If you can, observe that the start and finish of your path will always be the bottom two corners of the house. This has to do with the fact that these are the only two vertices of "odd degree."
[This is called an Euler path, and we will prove things about it] (ch 7)

— Example 4: Donuts (more number theory, and generating functions: ch 3, 7)

(a) I have n donuts. If I split them up 2 ways, there is 1 left over, 3 ways there is 1 left over, and 5 ways there is 3 left over. How many donuts do I have?

I have 13, or 43, or 73, or 103, etc.

(b) Now if I have m donuts and I split them three ways I get zero left, and 6 ways I get one left. Is this even possible? No!

[We will study this concept, called the Chinese Remainder Theorem, in great detail] (ch 3).

(c) How many ways can I pick 3 donuts if I must pick at least 1 chocolate, an even number of glazed, and at most 2 powdered-sugar?

What is the coefficient of the x^3 term in the expansion of
$$\underbrace{(x+x^2+x^3)}_{\text{chocolate}}\underbrace{(1+x^2)}_{\text{glazed}}\underbrace{(1+x+x^2)}_{\text{powdered sugar}}\ ?$$
And why did I label the terms with donut flavors?

[We will study why these two problems are asking the same thing] (ch 7).

— Example 5: Rabbits (sequences and recursion: ch 2, 4, 7)

If two rabbits fall in love, then n days later the number of rabbits will be f_n, where $f_0=1$, $f_1=1$, $f_2=2$, $f_3=3$, $f_4=5$, $f_5=8$, etc.
The pattern is that $f_n = f_{n-1}+f_{n-2}$. This is called a recurrence relation. It so happens that another formula for f_n is
$$f_n = \frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^n - \frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^n.$$
[We will learn why! (it's not that bad, either!)] (ch 7)