Discrete Mathematics

Cryptography

Bonnie Saunders

CTTI Workshop: UIC

May 4, 2013

These slides are available on my homepage.

What is discrete mathematics anyway?

Discrete mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous. In contrast to real numbers that have the property of varying ”smoothly”, the objects studied in discrete mathematics - such as integers, graphs, and statements in logic - do not vary smoothly in this way, but have distinct, separated values.

What is discrete mathematics anyway?

Although there is no agreed-upon definition of discrete mathematics, there is a general agreement that discrete mathematics includes three important areas: combinatorics, iteration and recursion, and vertex-edge graphs. These three areas, according to the "Principles and Standards for School Mathematics" established by the National Council of Teachers of Mathematics, "should be an integral part of the school mathematics curriculum.

Installing Python 2.7.3

- If you have Windows, you can download and install the Python 2.7.3 package from www.python.org/download. Make sure you can run IDLE.
- If you use MAC OS X: (If you do not have OSX 10.5 or higher, other things may need to be done.)
  - Download and Install the appropriate Python 2.7.3 package from www.python.org/download
  - Choose the package appropriate for your OS X
  - In order for IDLE to run you should also install Active State Tcl 8.5.12. You can download it from the website www.activestate.com/activetcl/downloads.

More to Installing Python 2.7.3

In order to do modular arithmetic in Python, you will need to install a Python Package called cypari. Do this in two steps:

- Install Setuptools: go to pypi.python.org/pypi/setuptools follow the instructions appropriate for your situation.
- From a command line: type

  ```
  easy_install -f http://math.uic.edu/t3m/SnapPy-nest cypari
  ```

Workshop 2: More Cryptography

Workshop goals:

- Frequency analysis
- Vigenère Cipher
- Cracking Arithmetic ciphers
  - Additive
  - Multiplicative
  - Affine
- Some problems: How to find multiplicative inverses $\mod n$
- CCSS Mathematical Practice Standard #7:

  Look for and make use of structure.

Other Resources

cryptoclub.org This website is new and under construction so please be patient. To join a group, Click: Challenges. See the Join-a-Group link under My Group Messages. There are two groups of interest:

This group has a message board that has many of the messages in the Cipher Handbook

- GROUP ID 140
- PASSWORD cryptography

This group was made for CTTI teachers. You can post your own messages here.

- GROUP ID 143
- PASSWORD ctticrypto