Discrete Mathematics

Cryptography

Bonnie Saunders

CTTI Workshop: UIC

April 27, 2013

These slides are available on my homepage.

What is discrete mathematics anyway?

Lots of things, including:

- Discrete is the opposite of continuous.
- Mathematics for doing computer science
- Mathematics done on computers

What is discrete mathematics anyway?

To name a few topics . . .

- Combinatorics
- Logic
- Probability
- Statistics

- Graph Theory
- Iteration and recursion
- Game Theory
- Cryptography

What is discrete mathematics anyway?

The flavor is often . . .

- Meaningful applications
- Easy to understand problems
- Fun and engaging

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 1: Classic Cryptography

Workshop goals:

- Caesar Cipher
- Arithmetic ciphers
  - Additive
  - Multiplicative
  - Affine
- Take a deeper look at the mathematics of arithmetic ciphers
- CCSS Mathematical Practice Standard #7:
  Look for and make use of structure.

Workshop 1: Classic Cryptography

Other Resources: cryptoclub.org