Ben Blau

Summary of CS235

These homework assignments contain python constructions of various mathematical processes that manipulate sets of data in various ways. This course had a large focus on constructing functions that would handle modular arithmetic as well as a focus on manipulating and generating data according to various desired properties. Most work was based around modular arithmetic and working with tuples. Several algorithms were used or provided throughout the assignments in order to complete the requirements.

The original assignments may still be found at <http://cs-people.bu.edu/lapets/235/s.php#assignment1> (adjusting the link for each assignment number). Please see the link if you wish to see a more in depth explanation of the topics covered. Below are a series of simplified explanations of various concepts covered throughout the assignments; however, not all topics are included below due to the amount of material covered. Information listed below is just an attempt to provide a simplified description of a majority of the topics covered in the course.

Assignment 1: Determination of perfect squares, square proper factors, determining certain shared properties such as reflexivity, symmetry, transitivity, and equivalency.

Assignment 2: Certain manipulation of specific data. Determining if values are prime and coprime. Construction of simple “random” number generators. Generating primes.

Assignment 3: Working with modular arithmetic. Determining inverse primes. Using an ecgd algorithm to solve systems of equations involving congruence classes.

Assignment 4: This assignment worked with solving various cases of equations including congruence classes. Implementing different components of the RSA cryptographic protocol. Computing square roots of congruence classes. Working with and determining square roots of tuples.

Assignment 5: Computing final compositions of permutations of similar forms to: [3,4,5,0,2,1] o [5,4,3,1,0,2] = ?. Creating functions that applies specific permutations to specific lists of data. Computing multiplication-induced permutations. Making a sort algorithm that works with cyclic permutations and multiplication-induced permutations. Working with modular multiplication. Creating a function that determines isomorphism.

Assignment 6: More work solving different forms of equations including modular arithmetic. Determining certain subsets of values returned through the required methods of solving the given equations. Solving systems of equations, using the linear congruence theorem, to produce different required results such as unique solutions and all sets of solutions.

I included various test cases throughout the assignments. These are not necessary for the assignments to function - they were only used to test various functions.