Jess Conway & Pranjali Mishra
March 13, 2018
COMP 460; Sekharan
Midterm Project Design Document

Part I, Planning:

Our project is designed to implement a set of Number Theoretic Algorithms on CPU/GPU. The first algorithms we would like to focus on are algorithms that deal with primality testing, semi-primality testing, and factoring. We have already completed programs that implement the Miller-Rabin primality test and semi-primality testing using Miller-Rabin, so this puts us in a good position thus far. There are several potential "next steps" for us to take, but we hope to discuss our project with Dr. Sekharan before moving forward with either one so that he can recommend which path we take first. The most obvious options are to move on to other algorithms, or to attempt to multithread our existing programs. If we do plan to move on to other algorithms before multithreading our existing code, we plan to attempt some advanced factoring algorithms next. But we have a number of other algorithms that may also be of interest. These topics include efficient algorithms for finding the Greatest Common Divisor (GCD) of two numbers, algorithms that solve 0/1 Matrix Problems, and algorithms that deal with Elliptic Curves. These will also be approached in an order that's recommended by Dr. Sekharan. Finally, once we are comfortable with the implementation of these algorithms on an ordinary CPU, we will turn to GPU programming to make the algorithms even more efficient.

Part 2, Code:

All of the code that we have so far has been attached in project/code. Currently, that includes one file that runs the Miller-Rabin primality test, one file that tests for Semi-Primality using Miller-Rabin and then brute-force tactics, and a third Driver file that allows for testing of both files simultaneously. There is a README file that explains how to use the Driver.java file for testing.

Part 3, Project Roles:

Jess Conway — Project lead. Wrote all code that has been completed thus far and is performing some research on GPU programming.

Pranjali Mishra — Has been researching both Number Theoretic Algorithms and GPU programming, but has been unable to contribute to the actual programming due to extended absence.