Master's Defense
Defense

Primality Testing and Integer Factorization Using Elliptic Curves

Andrew Wilson
Emory University

Abstract: Testing integers for primality and factoring large integers is an extremely important subject for our daily lives. Every time we use a credit card to make online purchases we are relying on the difficulty of factoring large integers for the security of our personal information. Similar encryption methods are used by governments around the world to protect their classified information, stressing the importance of the subject of primality testing and factoring algorithms to both personal and national security. Elementary number theory has been a key tool in the foundation of primality testing and factoring algorithms, specifically the work of Euler and Fermat, whose developments on modular arithmetic give us key tools that we still use today in the more complex primality tests and factoring methods. More recently people have used deeper ideas from geometry, namely elliptic curves, to develop faster tests and algorithms. In this thesis we continue this trend, and develop new primality tests that utilize previous theory of elliptic curves over finite fields. The primary point is that the points on these curves form a special group, which breaks down when working over Z/NZ, when N is not prime. Our theorems make use of the work of Kubert, Hasse, Mazur, and many more to yield a primality test that gives no false positives.

Thursday, April 6, 2017, 4:15 pm
Mathematics and Science Center: E406

Advisor: Ken Ono

Mathematics and Computer Science
Emory University